QUANTUM CRYPT

ENHANCEMENT OF AGT COMMUNICATIONS SECURITY USING QUANTUM CRYPTOGRAPHY

Work Package I — page 5
Work Package II — page 71
Work Package III — page 103

ENST/EEC/QC.12.01.WP3.A

Michel RIGUIDEL

Ecole nationale supérieure des télécommunications
Network and Computer Science department
46 rue Barrault, 75013 Paris, France.

Phone: +33 (0) 1 45 81 78 70
Fax: +33 (0) 1 45 81 71 58
Email: riguidel@enst.fr

January 5, 2005

© European Organisation for the Safety of Air Navigation (EUROCONTROL), June 2004.

This document is published by EUROCONTROL in the interests of the exchange of information. It may be copied in whole or in part, providing that this copyright notice and disclaimer are included.

The information contained in this document may not be modified without prior written permission from EUROCONTROL. EUROCONTROL makes no warranty, either implied or express, for the information contained in this document, neither does it assume any legal liability or responsibility for the accuracy, completeness or usefulness of this information.

Contents

I ATN and QKD Technologies **5**

WP1 Summary and Conclusions **7**

1 AGT Security Overview **11**
1.1 Why Security ? . . . 11
1.2 AEEC Ad Hoc Meeting on DLK Security . . . 12
1.3 ATN SARPs . . . 12
1.4 APIM 02-002 . . . 14
1.5 ATN Security Overview . . . 14
1.6 Conclusions . . . 15

2 Aeronautical Telecommunications Network **17**
2.1 ATN Overview . . . 18
2.2 CNS/ATM-1 Applications . . . 19
2.3 ATN Security . . . 20
2.4 Key Management . . . 21
2.5 ATN and IPv6 . . . 22
2.6 Air Identification Tag . . . 23

3 Quantum Key Distribution **25**
3.1 Why is Quantum chosen for Cryptography? . . . 25
3.1.1 Weakness of classical cryptography . . . 25
3.1.2 Appearance of Quantum Cryptography (QC) . . . 26
3.2 Quantum Key Distribution - QKD . . . 26
3.2.1 Principles of QKD . . . 26
3.2.2 Some protocols for QC . . . 27
3.3 Detailed BB84 protocol . . . 29
3.3.1 Description of protocol . . . 29
3.3.2 Security of BB84 . . . 31
3.3.3 Specification for a simple implementation of BB84 . . . 37

4 Free Space and Satellites **45**
4.1 Free Space . . . 45
4.1.1 State of the art . . . 46
4.1.2 The most recent success . . . 47
4.2 Satellites Communication . . . 50
4.2.1 Overview of satellites communication . . . 50
4.2.2 Satellites Free-space Communication . . . 54

5 Analysis and Scenarios **57**
5.1 Introduction . . . 57
5.2 Key exchange scenario . . . 58
5.2.1 The ground station transmits a key to the satellite . . . 59
5.2.2 The satellite transmits a key to the ground station . . . 61
5.2.3 The ground station transmits a key to another ground station using the satellite as a mirrror . . . 63
5.3 Satellite network . . . 66
5.3.1 Ground-Based Transmitter Terminal . . . 68
5.3.2 Space-Based Transmitter Terminal . . . 69

II ATN and QKD Scenarios **71**

Summary and Conclusions **73**

6 Introducing QC in ATN **75**
6.1 ATN Communications secured with PKI . . . 75
6.2 Scenario of QKD in ATN . . . 78
6.2.1 QCKI for A/G Applications . . . 79
6.2.2 QCKI for G/G Applications . . . 88
6.2.3 A proposal QKCI for ATN Network . . . 90

7 QC Communication Protocols **93**
7.1 Introduction to Communication Protocols . . . 93
7.1.1 Classical Authentication . . . 95
7.1.2 Quantum Authentication . . . 97
7.2 Quantum Authentication Protocol . . . 98
7.3 Communication protocols . . . 100

III Visual Demonstrators **103**

Summary and Conclusions **105**

8 AIT/QKD Animations in Flash **107**
8.1 Installation . . . 107
8.2 Opening `index.html` . . . 107
8.3 Air Identification Tag - AIT . . . 108
8.4 Quantum Key Distribution . . . 108
8.5 Flight plan and ATN . . . 108
8.6 Authentication and Integrity . . . 108

9 BB84 Demonstrator in Java **113**
9.1 Program installation . . . 113
9.1.1 For users on Unix, Linux or MacOS . . . 113
9.1.2 For users on Windows . . . 114
9.2 How to run simulator . . . 114
9.2.1 For users on Unix, Linux or MacOS . . . 114
9.2.2 For users on Windows . . . 114
9.2.3 The application is running . . . 114

Acronyms **121**

Index **129**

Bibliography **131**

WP I

ATN and QKD Technologies

Summary and Conclusions

The security of aeronautical telecommunication has become a crucial matter. Aeronautical telecommunication may be secured using classical cryptography. Classical cryptography provides so-called *cryptographic security*. That means that the security relies on the assumed difficulty of some mathematical problems.

On the other side, *Quantum Cryptology* (QC) provides unconditional security relying on the quantum physics law. Such a security is called *information-theoretic* security because it is proved using the theory of information. In this work, we study if Quantum Cryptology can be applied in the frame of the Aeronautical Telecommunication Network.

This part summarizes the partial conclusions of this first step study. These conclusions are partially made explicit and explained in the following sections.

AGT & ATN

The section 1 on page 11 is an overview of *AGT Security* and the section 2 on page 17 briefly describes the *Aeronautical Telecommunications Network*.

- All aeronautical communications are, or will be, handled by *Aeronautical Communications Network* (ATN). The ATN is an Internet network and may switch to IPv6 in the future.
- Security and confidentiality of communications are primary concerns. This is true for the ATN and for all aeronautical communications in general.
- Security and confidentiality in the ATN will be handled using public key cryptography. But public key cryptography is not proven to be unconditionally sure.
- Public key cryptography necessitates a *Public Key Infrastructure* (PKI). PKI are heavy administrative tools. Any failure compromises the system. PKI is likely to be applied in a well-trusted operators area such as European countries.
- *Air Identification Tag* (AIT) proposed by Eurocontrol (EEC) enforces security by allowing automatic digitalized identification without modifying current communication installations.
- Any solution for improving security must be done inside the framework of the ATN. It must consider costs and existing infrastructure into account. Existing infrastructure must be re-used.

© Eurocontrol, June 2004.

Quantum Key Distribution (QKD)

The section 3 on page 25 describes the Quantum Cryptology principle as described in its initial design called BB84.

- *Quantum Cryptography* (QC) uses classical encryption algorithms such as DES or AES.
- The main strength of QC is the *Quantum Key Distribution* (QKD) mechanism which allows to distribute the encryption keys.
- *Confidentiality* of QKD is ensured by the quantum physics laws, not by the assumed, but unproved, intractability of some mathematical problems.
- *Authentication* in QC is realized using special algorithms protected against key exhaustion by *Denial of Service* (Dos) attacks. However, a shared authentication key is still necessary.

Free space and Satellites

It must be pointed out that the current state of the art of Free Space Quantum Cryptology is extremely volatile because the technology and the theory are evolving quickly. This is mainly due to the funded research projects in Europe and USA.

QKD uses a quantum channel which may be an optic fiber or a free space laser beam. The section 4 on page 45 studies the use of free space QC and satellites for the distribution of encryption keys.

- Free space QC technology is rapidly evolving:

Year	Distance	Condition	Where
1989	32cm	Laboratory	IBM T.J. Watson (USA)
1996	150m	Day light	Baltimore (USA)
1998	1km	At night	Los Alamos (USA)
2000	1.6km	Day light	Baltimore (USA)
2001	1.9km	At night	QinetiQ (UK)
2002	10km	Day light	Los Alamos (USA)
2003	23.4km	At night	Germany

- 2km Ground/Ground QC is equivalent to 300km Ground/Space QC.
- Theoretical results with the 2003 technology allow a 1600km distance.
- Ground/Space QC requires high standards expensive opto-electronics and *pointing acquisition and tracking* apparatus.
- Actual free space QC requires huge flexibility in the receiver due to active polarization control and data analysis. Thus receiver is likely to stay on Earth.
- Actual free space technology relies on photons beams which are sensible to weather conditions. Further technologies may use different particles.

 © Eurocontrol, June 2004.

Analysis and Scenarios

The section 5 on page 57 studies what can be done with free space and satellite technology.

- There are three possibilities, each with its requirements and characteristics. As stressed earlier, the better is to keep the receiver on earth. The three possibilities are:
  - The ground station transmits a key to the satellite.
  - The satellite transmits a key to the ground station.
  - The ground station transmits a key to another ground station using the satellite as a mirror.
- Average embedded payload is 5kg with a 10 to 30cm optics. On Earth, it uses a 50 to 100cm optics.
- The size of the satellites network depends on the chosen payload and varies from 7 to 43 satellites.

Partial Conclusions

- Any improvement in AGT security must be done inside the framework of ATN and must not be too expensive. Improving key distribution inside ATN may be considered as admissible.
- Coupling QC with AIT may also be considered as admissible. For instance, AIT may be coupled with QC Authentication algorithm to provide a secure identification.
- Using PKI for key distribution is not proven to be secure. One may find a way, or may already have found, a way to break it. If Quantum Computers are built, PKI is considered as broken since algorithms for these computers allow to break it.
- Quantum Key Distribution is the only key distribution scheme which is proven to be secure using the quantum physics laws. QKD authentication is not subject to key exhaustion by Denial of Service attacks.
- Free Space Quantum Technology for Ground/Plane, Ground/Satellite and Plane/Satellite key distribution is not ready. Theoretical results allow such a technology which may be ready in 10 years according to current progress records. Current technology allows admissible payload either in aircraft or satellites.
- The most foreseeable plan would be to use satellites-based key distribution. The required number of satellites varies from 7 to 43 depending on the evolution of technology. It is a costly solution which may be used only if PKI is broken by Quantum Computers or mathematical progress.

© Eurocontrol, June 2004.

WP2 Future Works

- To provide a visual demonstrator of BB84 protocol.
- To develop several satellite-based scenarios with the following constraints and questions:
  - Is it possible to incrementally inject QC inside the ATN PKI ?
  - Is it possible to use QC for specific links only such as VHF/AIT links ?
  - Is there some environmental impact ?
  - Is there some public health concern ?
- To provide visual demonstrators for the preceding scenarios.

 © Eurocontrol, June 2004.

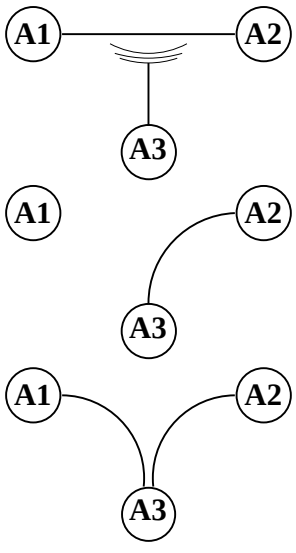
Section 1

AGT Security Overview

Informations from this section are mainly provided from [29]. It is a short description of the state of the art in *Air Ground Telecommunications* AGT Security and a short description of the institutional concerns.

1.1 Why Security ?

AGT Data Link (DLK) provides numerical communications between ground stations and aircraft. These communications are used for Graphical Position Reports, Contact Reports, etc. One may classify different threats on Data Link communications:



Monitoring. A third party may listen to the Data Link communications and gain informations on the traffic.Current Data Link communications do not guarantee *privacy*.

Spoofing. A third party may listen to the Data Link communications and gain *authentication* informations in order to impersonate one of the parties.

Modifying. A third party may impersonate the second party with respect to the first party meanwhile he may also impersonate the first party with respect to the second party (*man-in-the-middle* attack). *Integrity* of the data is not preserved. Data may be corrupted.

Main sources:

[15] http://www.arinc.com/aeec/projects/users_forum/Miami_03/6-3_Ad Hoc Security Report - Exec Summary.pdf

[29] http://www.arinc.com/aeec/projects/users_forum/Miami_03/6-2_ATN Security - USAF.pdf

[44] http://www.arinc.com/aeec/projects/users_forum/Miami_03/6-6_APIM-ATN Security.pdf

[6] http://www.arinc.com/aeec/projects/users_forum/Miami_03/6-4_Key Management.pdf

© Eurocontrol, June 2004.

It is very easy to monitor *Aircraft Communications Addressing and Reporting System* (ACARS) Data Link Messages. One needs:

- A personal computer.
- A sound card
- A *Radio Frequency* (RF) scanner.
- Few software available on the WEB.

1.2 AEEC Ad Hoc Meeting on DLK Security

The meeting was held in Columbia (Maryland,USA) from 7 to 9 may 2002 and was hosted by Honeywell.

There were many presentations by the interested agencies which are looking at security concerns. All meeting attendees agreed that it is time to look at standards of development for AGT security. They emphasized that opportunities exist for *Data Link Service Provider* (DSP).

ATN security remains the baseline. ACARS security must be compatible with *Aeronautical Telecommunications Network* ATN (cf. section 2 on page 17), security requirements. One must not build an ACARS only solution.

Analysis 1.2.1. *This is a very important point: a security solution must be compatible with the future ATN.*

The main conclusions of the meeting were:

- Security of Data Link communications is a serious concern.
- There exists a problem with the open distribution of threat and vulnerability informations.
- A ACARS solution compatible with ATN security has to be found.
- Minimizing costs of a solution is a concern.

1.3 ATN SARPs

ATN Standards and Recommended Practices is documented by ICAO Document 9705 (third edition), Sub-Volume 8, October 2002. ATN SARPs is based on the following elements:

- Eurocontrol has performed a risk analysis and has identified the following threats and vulnerability:
  - Modification and replay of AGT.
  - Denial of services by flooding routing databases.
- Airlines require confidentiality of operational data.

 © Eurocontrol, June 2004.

ATN SARPs provides the following security services:

- Authentication and integrity of Air-Ground Telecommunications.
- Authentication and integrity of IRDP (*Inter-Domain Routing Protocol*) communications.
- Supporting Public Key Infrastructure (PKI).

Note that the ATN Panel (ATNP) WG-B/Sub-Group 3 is enhancing the ATN SARPs with confidentiality services.

The SARPs document is organized as follows:

- 8.1 - Introductory Materials.
  - 8.1.1 - ATN Security Services.
    - Support operational requirements of secure exchange.
    - Support mobile and fixed network users.
  - 8.1.2 - ATN Security Services Providers.
    - Message assurance from originator.
    - Authentication by receiving entity.
- 8.2 - General ATN Security Concept and Services.
- 8.3 - ATN Security Framework.
  - Standards.
  - Provision of Security Services.
  - ATN Physical Security Framework.
- 8.4 - ATN Public Key Infrastructure (PKI)
  - Certificate Policy.
  - Certificate Format.
  - Certificate Revocation List (CRL) Format.
  - Certificate and CRL Validation process.
- 8.5 - ATN Cryptographic Infrastructure.
  - Key Agreement.
  - Digital Signature.
  - Message Authentication.
- 8.6 - ATN System Security Object.
- 8.7 - ASN.1 Module for ATN Security.

[29] quotes the following sentences from the ICAO SARPs, section 8.1.2 notes: *Security services in general support but do not guarantee protection from security violations ... Cryptanalytic advances may affect the overall level of protection.*.

Analysis 1.3.1. *The SARPs mentions that PKI-based security is not guaranteed and that it depends on advances in cryptanalysis. But it does not mention the possible birth of Quantum Computers. That is exactly the problems that Quantum Cryptography claims to solve.*

For instance; SARPs mentions that Key Pairs (public and private keys) must be changed every 28 days and that private keys must be protected. The fact that private keys must be protected is an evidence:

- If the private key of a Certificate Authority (CA) is disclosed, then the whole security system depending on the CA is broken.
- If the private key of an aircraft is disclosed, then anyone can impersonate the aircraft communication system.

Analysis 1.3.2. *One may worry about the 28 days key renewing delay. 28 days may be sufficient to crack a public key.*

1.4 APIM 02-002

The ARINC IA Project Initiation/Modification (APIM) 02-2002 named *ATN Security* results from the ICAO Air Navigation Bureau Request for Development of Specifications for Key Management and Distribution needed to implement the security provisions of ATN SARPs for avionics equipment.

One reason for the APIM is local implementation issues: everyone has to do it the same way or it will not work.

1.5 ATN Security Overview

The ATN Panel (ATNP) has provided mechanisms which may be applied for:

- Authentication and Integrity of Air-Ground application communications which use the ATN upper layers.
- Authentication and Integrity of Air-Ground IDRP, i.e. inter-domain routing protocol, communications.
- Authentication of Ground-Ground Applications communications, Ground-Ground IRDP and Aeronautical Message Handling Services (AMHS).

The used technologies are rather classical:

- HMAC: Hybrid symmetric, Hashed Message Authentication Code.
- ECDSA: Elliptic Curve Digital Signature encryption Algorithm.
- GULS: ISO Generic Upper Layer Services.

 © Eurocontrol, June 2004.

- CMA: Context Management Application to manage mutual authentication during initial contact.

The message costs are the following:

- CMA initial contact:
  - Logon request: 400 bits.
  - Logon response and certificate: 1500 bits.
- Subsequent secured message: 32 bits (Message Authentication Code).

Note that efforts have been made to minimize the costs. For instance, a X.509 certificate is about 20 KB.

The Certificate Delivery Services delivers certificates and Certificate revocation Lists (CRL) to ATN entities. X.500 directory is likely to help on the ground.

- Ground scenarios:
  - Applications and routers have directory access.
  - CMA has directory access and provides certificates and CRL.
  - Certificates are pre-stored at initial deployment.
- Air scenarios:
  - Short-lived certificates sent to aircraft.
  - CMA certificates pre-stored at initial deployment.

Analysis 1.5.1. *An eavesdropper accessing the pre-stored certificates may endanger the security system.*

1.6 Conclusions

Analysis 1.6.1. *Any solution, any addition or improvement to the security must be done in the frame of the ATN construction. It must be fully compatible with ATN.*

Analysis 1.6.2. *ATN Security relies on very classical technologies which have been mapped to the particular structure of ATN. Such technologies are not fully-proved to be sure.*

Section 2

Aeronautical Telecommunications Network

In 1983, the *International Civil Aviation Organization* (ICAO) created the Special Committee for *Future Air Navigation Systems* (FANS) for studying new concepts and new technologies and making recommendations for the future of air transportation.

FANS emphasized the need for interchange of digital data over several data links. It recommended the *Open Systems Interconnection* architecture (OSI) from the *International Organization for Standardization* (ISO).

FANS's work ended in 1988 with the proposition of the *Communication, Navigation and Surveillance* (CNS) concept to help the development and evolution of *Air Traffic Management* (ATM).

In 1989, the *Air Navigation Commission* (ANC) included the development of ICAO material for the interoperability between all *Air Traffic Services* (ATS) Data Link to the *Secondary Surveillance Radar Improvements and Collision Avoidance Systems* Panel (SISCASP) which were already responsible of the Surveillance and *Traffic Alert/Collision Avoidance System* (TCAS).

The SISCAS Panel proposed the concept of *Aeronautical Telecommunications Network* (ATN) which were first published as an ICAO manual in 1991 and then completed in 1993. The *Standards and Recommended Practices* (SARP) and *Guidance Material* (GM) were published in 1997. ATN was described as an Internet network based on classical OSI protocols supporting global communications and all ICAO Air-Ground Data Links.

Main sources:

[15] http://www.arinc.com/aeec/projects/users_forum/Miami_03/6-3_Ad Hoc Security Report - Exec Summary.pdf

[29] http://www.arinc.com/aeec/projects/users_forum/Miami_03/6-2_ATN Security - USAF.pdf

[6] http://www.arinc.com/aeec/projects/users_forum/Miami_03/6-4_Key Management.pdf

© Eurocontrol, June 2004.

Other ICAO Panels were involved in the ATN:

- The *Aeronautical Mobile Communication* Panel (AMCP) which domains of interest are *Aeronautical Mobile Satellite Services* (AMSS), *High Frequency* (HF) *Data Link* and *Very High Frequency* (VHF) *Data Link* SARP.
- The *Automatic Dependent Surveillance* Panel (ADSP) which domains of interest are the Ground/Ground and Air/Ground CNS/ATM operational requirements.
- The *Aeronautical Fixed Service and System Planning* Panel (ASPP) which domains of interest are the Ground/Ground communications, including *Aeronautical Fixed Telecommunications Network* (AFTN) and *Common ICAO Data Interchange Network* (CIDION), and *Aeronautical Message Handling Systems* (AMHS) SARP.

Since 1994, the ATN SARP's is under the responsibility of the *Aeronautical Telecommunications Network* Panel (ATNP). It is organized in five parts:

1. Introductory material.
2. Air/Ground applications: *Automatic Dependent Surveillance* (ADS), *Controller Pilot Data Link Communications* (CPDLC), *Flight Information Services* (FIS) and *Context Management* (CM).
3. Ground/Ground applications: *Inter-Centre Communications* (ICC), *Aeronautical Message Handling Service* (AMHS).
4. *Upper Layer Architecture* (UAL).
5. Internet: Network and Transport Layers.

The three other ICAO Panels (AMCP, ADSP, ASPP) are also involved in the development of ATN.

2.1 ATN Overview

The ATN is a data communication network.

- It provides a common communication service for all *Air Traffic Services Communication* (ATSC) and *Aeronautical Industry Service Communication* (AINSC). Communications can be either Ground/Ground or Air-Ground;
- It integrates and uses existing communication networks and infrastructure if possible. Investments in existing leased networks, CIDIN and X25 networks must be preserved.
- It must meet security and safety requirements of ATSC and AINSC applications and accommodate the different levels of service required by each ATSC and AINSC application.

 © Eurocontrol, June 2004.

- It must provide ATN users with a robust and reliable communication service. Its design ensures high availability because there is no single point of failure and because it permits multiple alternative routes to the same destination with dynamic switching between alternatives, for both fixed and mobile communication.
- It must support mobile systems since an aircraft is basically mobile. It must support a wide variety of mobile communication networks including AMSS, VDL and Mode S. It must be possible for any system to communicate with an aircraft equipment all over the world.

The services provided by the ATN are implementing the *OSI Transport Service* referred as ISO 8072. In order to build ATN applications, ATN proposes common functional components in an architecture known as the *Upper Layer Architecture* (ULA) based on the layered OSI Reference Model. There exist seven layers. Two types of entities are identified:

- *End systems* such as computers using the 7 layers.
- *Intermediate systems* such as routers using the 3 lower layers.

The seven OSI layers are listed below from the upper to the lower:

- The *Application Layer*. Semantics of end-to-end exchanged information.
- The *Presentation Layer*. Syntax of end-to-end exchanged information.
- The *Session Layer*. Format of end-to-end exchanged information.
- The *Transport Layer*. End-to-end flow control and information exchange.
- The *Network Layer*. Establish, maintain and terminate switched connections.
- The *Data Link Layer*. Synchronization and error control over the physical link.
- The *Physical Layer*. Management of the physical link.

The three upper layers provide common functions that are used for the establishment and release of connection and for the encoding of information.

2.2 CNS/ATM-1 Applications

The *Communications, Navigation and Surveillance / Air Traffic Management* Applications that has been specified for the first phase of ATN:

- *Context Management* (CM) provides a mean to find out communications services within a given flight region, and for a ground system or controller to direct an aircraft's Context Management Application to contact a different flight region.

- *Automatic Dependent Surveillance* (ADS) is designed to give automatic reports from an aircraft to a ground system. This information is provided on demand and in an emergency. Aircraft position and trajectory and meteorological data are typical uses of this service.
- *Controller-Pilot Data Link Communications* (CPDLC) provides a mean for two-way message oriented communications including a set of clearance/information/request messages corresponding to current voice phraseology employed by ATC procedures.
- *Flight Information Services* (FIS) can support a variety of information services, providing information about the ground to an aircraft. This can include information about an airport, such as runways in use and weather conditions.
- *ATS Interfacility Data Communication* (AIDC) provides a mean for the exchange of ATC information between Air Traffic Services Units in support of ATC functions, including notifications of flights approaching a Flight Information Region boundary, co-ordination of boundary crossing conditions, and transfer of control.
- The *Aeronautical Message Handling System* (AHMS) provides a mean for the exchange and distribution of message oriented traffic between Air Traffic Services Units. It is an AFTN replacement that may be used additionally to provide new messaging services including Electronic Mail and Electronic Data Interchange. It is based on ITU recommendation X.400 .

See `http://www.helios-is.com/atn/atnover/S59577.htm` for more details.

2.3 ATN Security

As a result of study done by Eurocontrol[1], it is suggested that the following are threats against the ATN, including ATN management and application services, which pose a significant threat to which the ATN is vulnerable, and hence require specific counter-measures:

1. To Air Traffic Control Messages, both Air/Ground, and Ground/Ground, there are threats resulting from:
   - Modification
   - Replay
   - Masquerade
   - Jamming
2. To X.400 Message Handling System (MHS), there are threats resulting from:
   - Modification
   - Masquerade

[1] Cf. `http://www.helios-is.com/atn/atnover/S59616.htm`

 © Eurocontrol, June 2004.

3. To OSI Systems Management:
   - Modification
   - Replay
   - Masquerade
   - Unauthorized modification of management information base
4. For all applications, vulnerabilities exist to Denial of Service attacks on the ATN which impact Air Traffic Control Messages including:
   - Jamming air-ground links
   - Flooding the ATN with data packets
   - Causing switches and data links to fail.
   - Unauthorized modification of routing information.

These are to be addressed by network design and topology, and physical access security, which should be considered by regional planning bodies, and by appropriate mechanisms implemented by the ATN Internet.

As a result of this work, it is believed that application messages need to be protected by *digital signatures* providing both authentication of the sender and a high quality data integrity check. Furthermore, the source of routing information needs also to be similarly authenticated.

We can summarize the Security Requirements for ATN:

- Authentication of Message Source
  - protect against misreporting
  - protect against masquerade of controllers
- Message Integrity Check
  - protect against message substitution
  - protect against message replay
- Authenticate source of routing information
  - protect against false route

2.4 Key Management

[6] mentions: ICAO ATN Panel sent a letter inviting AEEC to develop specifications for Key Management in ATN. Reference: ICAO ATN SARPS 9705 Ed. 3. The elements of the ICAO request are:

- ATNP needs a suitable mechanism for secure installation and update of the aircraft private keys in the context of data link information security.
- ATN security mechanisms require support of a Public Key Infrastructure (PKI).

- There is a need for secure installation and update of aircraft private keys as well as public keys of other avionics.

Analysis 2.4.1. *One of the main security problems of ATN is the delivery of encryption keys, as in any secured system.*

A PKI is a key management system composed of trusted entities named *Certificate Authority* (CA). CA builds and delivers authentic digital public key certificates, normalized as X.509 certificates, binding an *identity* with a public key. They must emit *Certificates Revocation Lists* (CRL) when certificates are revoked. There is no standard concerning PKI and most of them are not interoperable.

Analysis 2.4.2. *PKI relies on public key.encryption which, in turn, relies on some unproven intractable mathematical problems such as factoring large numbers. A few remarks:*

- *Such problems may be already solved by a mathematician whose rough interest is not to publish its result but to sell it to NSA, Al Quaeda, etc.*
- *Such problems may be solved by heuristics, i.e. algorithms which may fail in some cases and succeed in some other cases.*
- *Such problems are definitively solved by the future (30 years?) Quantum Computers.*

In [6], it is mentioned that there will be *State Certificate Authority*, that is CA assigned by states (e.g. USA assigns FAA or Europe assigns Eurocontrol) and that such CA's must establish trust relationships. CA authorities issue certificates to ATN entities. Then there exists *Operating Agency Certificate Authority* (OACA), for instance airlines, which are subordinated to the CA and issue certificates to aircraft within their domains.

When one wants to check a certificate, one does it with the public key of the corresponding OACA. Then one can check OACA certificates with the public key of its CA.

Analysis 2.4.3. *Moreover, the secrecy and the validity of the certificates rely on the security of the whole PKI infrastructure. If one CA or OACA private key is stolen, the PKI system is broken.*

2.5 ATN and IPv6

The ATN is an Internet network with fixed and mobile elements. Such a network is managed using protocols. Most of today's Internet is managed using IPv4, *Internet Protocol Version 4*. However, the *Internet Engineering Task Force* (IETF) has designed *Internet Protocol Version 6* (IPv6), the next generation Internet Protocol. IPv6 fixes a number of problems existing for IPv4 such as the absence of *Quality of Service* (QoS), IPv4 only supports *Best Effort*, or the shortage of available IP addresses.

For instance, IPv4 addresses are limited to 32 bits. It was sufficient 25 years ago. However, addresses are allocated by classes and much of the "big" classes

 © Eurocontrol, June 2004.

are allocated to US providers. IPv6 has a 128 bits address space allowing 3.4×10^{38} possible IP addresses. Every square centimeter on earth can be individually addressed using IPv6. Internet programs such as *Network Address Translator* (NAT), allowing to hide a sub-network behind one IP address with some drawbacks, are not needed any more.

IPv6 has built-in security services. The support of IPSec is mandatory. IPv6 has support services for mobility with neighboring discovery mechanisms. IPv6 also has support for *Quality of Service* (QoS). One element of these services is the presence of packet flow identification which does not exist in IPv4. Most of the operating systems, commercial and not commercial, now support IPv6 which can coexist with IPv4.

Some studies, for instance Eurocontrol iPAX, claim that ATN could use IPv6 because the expected number of aircraft using ATN in the next 25 years is over 100 000. Each aircraft is expected to have many equipments on board subject to be linked to the ATN. With its indecent number of available address, each equipment could have its own IP address. Moreover, IPv6 is claimed to be scalable to very large networks and it has supports for security and QoS. IPv6 is viewed as a possible enhancement of the ATN and an option for ACARS. IETF is working on new mechanisms for mobility (NEMO). IPv6 would need mobility mechanism that meets the ATH requirements, in particular concurrent use of multiple data links.

When OSI has been chosen for the ATN, it was the only network protocol that could meet most of the ATN requirements. However, OSI has not fulfilled the expectation that it would replace TCP/IP. IPv6 is still in its infancy. Since IPv6 and IPv4 can coexist, there may be a gradual shift from IPv4 to IPv6. Internet and telecommunications companies are interested and working to improve IP protocols and many investments are made into IPv6. Aeronautical companies could benefit of these investments.

2.6 Air Identification Tag

Air identification Tag (AIT) has been developed by the University of Graz (Austria) and Eurocontrol. It is described in *Eurocontrol Experimental Center* (EEC) Innovative Research activity report for year 2003.

Controller-pilot *Very High Frequency* (VHF) voice communications in *Air Traffic Control* (ATC) relies on amplitude modulation by a carrier frequency. Pilots have to identify themselves with their call-signs. Human imperfections in speaking and hearing added to the poor quality of this communication channel may cause identification problems.

AIT aims at improving and facilitating identification. IT inserts automatically an unnoticeable small data-link channel in the communication. The inserted data can be a digital signature associated with the emitter and may be used to achieve reinforcement of audible stimulus with a visual stimulus.

To embed the data into the pilot's communication, AIT uses watermarking: the signal is digitalized, then the digital watermark is added and the resulting signal is converted to an analogical signal again. One can obtain about 200 bits/sec of embedded communications without modifying current airplane

AC equipment. The use of the pilot's *Push-To-Talk* (PTT) switch automatically inserts a digital signature in the communication. If the other party does not have the additional equipment, it will not interpret the watermark but the communication will not be perturbed. If the other party has the decoder then it interprets the signature and displays the aircraft identification.

AIT could be used to avoid oral misunderstanding of aircraft identification. But it can also be used for security purposes because it proposes a digital identification of the aircraft. Communication hack becomes much more difficult.

Analysis 2.6.1. *Aircraft digital signature for AIT could be distributed using Quantum Key Distribution.*

 © Eurocontrol, June 2004.

Section 3

Quantum Key Distribution

3.1 Why is Quantum chosen for Cryptography?

Information exchange is always an essential need in the human life, particularly in the nowadays modern society. The amount of information exchanged is increasing every minute, even second or smaller time unit. And it is unavoidable to take into account the importance of its secrecy. It concerns the confidentiality and integrity of data transferred. This was thought to be secured by classical cryptography techniques, for instance: symmetric/asymmetric key or both of them in today's best systems. However, in the age of powerful computers with developed technology of chip-processors at high speed (billion calculations per seconds), classical cryptography gradually reveals its weakness.

3.1.1 Weakness of classical cryptography

As we have known, almost all current cryptosystems generate keys for cipher (or decipher) messages using:

- a random choice from a set of possible values as in DES and its variants.
- or one-way functions which are considered difficult to reverse, as in Diffie-Hellman and RSA [13]. Time needed for reversing such functions is exponential in the input size.

For the former, we can think that it is safe when the key is randomly generated but it is not really possible to achieve random key generation, in principle, by using present deterministic, finite state computers. However, the situation is not better with one-way functions because, unfortunately, up to now nobody builds any proof that one-way functions are believably mathematically difficult to inverse. Moreover, Peter Shor discovered in 1994 that time to factor a large integer or calculate the discrete logarithm is polynomial if applying quantum computers. So the main cause which menaces today's cryptosystem is the really rapid development in quantum computer technology.

But no problem has no solution, duty is just to find out it. And a proposition for current cryptography is *Quantum Cryptography*.

© Eurocontrol, June 2004.

3.1.2 Appearance of Quantum Cryptography (QC)

In 1970, QC was firstly proposed by Wiesner in his paper which had not been published until 1983 (appeared in [SIGACT News 15 no.1]). And QC helped the scientists to open the door for the application of quantum information theory, which itself is founded on the fundamental axioms of quantum physics.

More detailed, QC provides a secure protocol to exchange cryptographic keys. This protocol is called quantum key distribution or quantum exchange.

3.2 Quantum Key Distribution - QKD

3.2.1 Principles of QKD

The quantum key exchange is based on two physical theorems which help to generate a secure key between Alice and Bob. They are the no-cloning theorem and uncertainty principle [37].

- *uncertainty principle*: this is one of the fundamental principles in quantum mechanics which says that if the measurement used is incompatible with the unknown state prepared, so it will interfere the original one of the system.
- *no-cloning theorem:* based on the *uncertainty principle*, there is no way to know a state for sure. And cloning an unknown state is impossible, we cannot have a perfect copy of a random quantum state.

In comparison with traditional cryptography key distribution, QKD can solve some shortcomings. Besides strong points, QKD also has some some weak points mentioned below.

Advantages of QKD

As mentioned in the precedent part, QKD is based on quantum mechanics. The main strong point of QKD is that it ensures the *confidentiality of keys* guaranteed by the quantum physical laws. This is the major reason why QKD is favored. QKD techniques can provide automatic distribution of keys that offers a greatest security than classical ones. The Quantum properties used in QKD are:

- *Entanglement (quantum correlation).* A quantum system may be correlated with one or more quantum systems. Each sub-system generates randomly its states, and none of them has a fixed state.
- *Causality and superposition.* Causality is not an ingredient of non-relativistic quantum mechanics. Nevertheless it is used for the aim of combination with superposition used for secret key exchange.

 © Eurocontrol, June 2004.

Shortcomings of QKD

- *Authentication.* When exchanging the secret data, one must pay attention a lot to address the right destination. It is a pity that authentication is not primitively included in QKD. This problem is being studied to improve QKD and has opened some approaches such as including the secret key in the distant devices or hybrid QKD-public key schemes.
- *Sufficiently rapid delivery of keys.* A rapid speed is taken into account when distributing keys. The reached order of today's QKD is about 1000 bit/s throughput for keying material, but in fact often runs much more times slowly [12].
- *Robustness.* It is really a weak point of QKD since it uses a single point-to-point connection. So, it can be easily weakened by an eavesdropper or by a possible accident like fiber cutting. However, it is unprobable if using multi-path for transmission of data.
- *Distance and Location Dependence.* We can clearly realize that QKD is notably short of this attribute. Two entities of a QKD system must have a dedicated connection and the distance between them is limited by the material used for transmit photons.
- *Resistance to traffic analysis.* Someone may enjoy to carry out traffic analysis on a key distribution, particularly on dedicated system which promises interesting things behind. It probably causes some risks. To ease the life, it should be preventing such analysis. Unfortunately, QKD cannot do that thing but attracts a lot the curious eyes by its dedicated setups.

3.2.2 Some protocols for QC

Up to now, there are several protocols being proposed since the birth of the first one BB84. We will summarize some of them in this section.

- **BB84 protocol**

  It is the first protocol for Quantum Cryptography, introduced by *B*ennet and *B*rassard in 19*84*, thus it was named *BB84*. In 1994, this protocol was proved to be secure against eavesdropping by Dominic Mayers, Eli Biham, Michael Ben-Or. BB84 is a *non-deterministic* protocol, which means that it is useful for distribution of a random sequence only. We will come back to this in detail in section 3.3 on page 29.

- **Two-state protocol**

  In 1992, according to Bennett's notice, four states are too much for QC, only two non-orthogonal ones are sufficient. In truth, the security of QC bases on the inability of an evildoer to distinguish surely and without perturbation the different states that Alice sends to Bob; hence two states are enough (Bennett, 1992) if they are incompatible (i.e., not mutually orthogonal). But in practice, this protocol is not really effective. Indeed,

although two nonorthogonal states cannot be distinguished unambiguously without perturbation, one can unambiguously distinguish between them at the cost of some losses (Ivanovic, 1987; Peres, 1988). This possibility has been demonstrated in practice (Huttner, Gautier, et al., 1996; Clarke et al., 2000). [37]

- **Three-state protocol**

  This protocol is to improve BB84. The BB84 protocol is symmetric in its use of polarization. After the generation of the key, it is necessary to exchange more other information for secrecy of the key. Is it possible not only to distribute the key but also to provide additional information about the integrity. Three-state protocol proposed to use three states, in place of four in BB84, and three detectors, instead of two for BB84, to break the symmetry of BB84. This reduces eavesdropping's probability to get right states, and also minimizes the amount of useful information received by Alice. Moreover, we can also discover her presence on the line.

- **Six-state protocol**

  While two states are enough and four states are standard, a six-state protocol better respects the symmetry of the qubit[1] state-space, see 3.2.2. The six states constitute three bases, hence the probability that Alice and Bob choose the same basis is only 1/3, but the symmetry of this protocol greatly simplifies the security analysis and reduces optimal information gain of the eavesdropper for a given error rate QBER[2]. If the eavesdropper measures every photon, the QBER is 33%, compared to 25% in the case of the BB84 protocol.

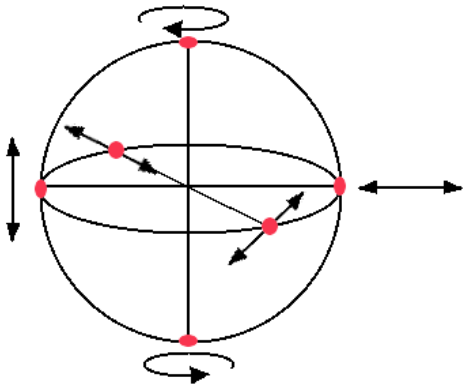


Figure 3.1: Three pairs of bases used in six-state protocol.

[1] Qubit: quantum bit.
[2] QBER: Quantum Bit Error Rate.

 © Eurocontrol, June 2004.

3.3 Detailed BB84 protocol

3.3.1 Description of protocol

BB84 is the most well-known quantum key distribution protocol using four different states that make a pair of basis states.

*In the description of the protocol, we use classical first name for the different elements of the protocol. The name **Alice** is used for the initiator of the protocol. The name **Bob** is used for the responder. Typically, Alice is communicating with Bob while an eavesdropper (a spy) is trying to listen or perturb the communication. This eavesdropper is usually named **Eve**.*

Secrecy of this protocol was proved by different people such as Dominic Mayers, Eli Biham, Michael Ben-Or and so on. BB84 is secure against eavesdropping in the sense that Eve can't gain any information about the transfer between Alice and Bob unless she reveals her presence after data transmission. We will come back to this item in the section 3.3.2 on page 31.

BB84 is a non-deterministic protocol. That means that it distributes random sequence of bits. BB84 cannot be used for the transmission of a determined message. Alice and Bob's communication being successful merely bases on the randomness at every stage of the protocol. Now, let's go to see how BB84 works.

The BB84 quantum coding scheme was the first proposed quantum encoding of classical information in such a way that the receiver (legitimate or illegitimate) cannot recover with 100% reliability. It constitutes a base that most others quantum protocols fund on.

With this scheme, classical bits are encoded by quantum states. Each quantum state can represent both classical bit, 1 or 0, and inversely, each 0 or 1 correlates (corresponds) to a mixture of two equally likely non-orthogonal quantum states. One of many representations is in figure 3.2 where we represent by $|0\rangle$, $|1\rangle$, $|0'\rangle$, $|1'\rangle$ the four states illustrated.

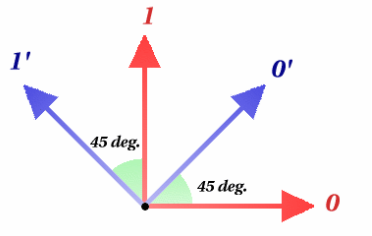


Figure 3.2: Non-orthogonal four states used in protocol BB84.

Information transmitted in the quantum channel is usually under the form of polarized photons. Encoding the classical bits is done using the direction of the polarization. In BB84 coding scheme, the classical bit 0 is represented by a photon polarized both $0°$ and $45°$ of horizontal axe, and the two corresponding orthogonal directions, $90°$ and $135°$, are used for bit 1.

According to quantum mechanics, there is no way to differentiate surely two non-orthogonal states. So a quantum measurement must be performed to determine the received state and from that to get the classical output. And this uncertainty principle provides cryptographic properties needed in quantum cryptography.

For BB84, there are two measurements used to distinguish the different quantum states:

- $\oplus$, measurement allowing to identify clearly between two states $|0\rangle$ and $|1\rangle$. This measurement is also called *measurement in the rectilinear basis.*
- $\otimes$, measurement allowing to identify clearly between two states $|0'\rangle$ and $|1'\rangle$. This measurement is also called *measurement in the diagonal basis.*

In general, quantum key exchange using BB84 for secret key consists of six following steps:

1. *Quantum Transmission*
   This phase is the first step in a quantum key distribution. In this phase, a random string of n classical bits will be created by Alice and sent to Bob. Each bit of this string will be encoded by a non-deterministic basis. A quantum encoded classical bit is called a *qubit.* At the other side of the transmission, Bob receives the qubit and he picks up by chance a rectilinear (or diagonal) basis to measure it. When the transmission is over, Bob will get a string of classical bits, called the *raw key*, different from Alice's one in many positions, about 50% even in the case of error-free quantum communication or much more as apparatus error rate is included. The next step of the protocol will help to replace the uncorrelated (uncorresponding) bits between Alice's and Bob's string which are possible errors caused by either Eve or noisy quantum transmission.
2. *Bases Announcement*
   As mentioned in the previous part, in this phase, all the positions where the same bits are shared will be kept and the rest will be discarded. Firstly, using classical channel, Bob sends all the bases he used to measure Alice's qubit string to Alice. Alice then compares this sequence of bases with hers and discloses every uncorrelated positions to Bob over classical channel. After that, both Alice and Bob replace all the bits at positions informed by Alice. And the distilled part of raw key, called *plain key*, is totally the same between Alice and Bob regardless apparatus error but still or even quite different from each other in fact.
3. *Error Estimation*
   To reduce the difference between Alice's and Bob's plain key due to apparatus imperfection, it is necessary to correct errors. It is the phase in which the plain key error is estimated. It will be performed as follows. Alice will extract a small sequence of the plain key and send it to Bob. Alice will inform Bob a subset of positions of size K and the bit values at those positions in the raw key got in the last step. Both transmitter and receiver have to compute the observed error-rate e and keep this transmission if error rate is less than a desired threshold. And finally, they take away the K checked bits and observe the rest. In the case where the estimated error rate is more than the threshold, the key will be aborted.

 © Eurocontrol, June 2004.

4. *Reconciliation*
   After this phase, a *reconciled key* will be achieved after applying a reconciliation protocol to the plain key. Reconciliation is an interactive process taking place over the public channel. The purpose of this phase is to correct the errors, equivalently to reduce the difference, between sender's and receiver's plain keys. But it is important to take note that as few bits as possible are sent over the public channel since Eve may exploit this information. A protocol called *Cascade* is applied here. Cascade performs error-correction by sending very little information over the public channel and was proposed by Gilles Brassard and Louis Salvail. Cascade operates in a number of rounds. We will go in detail in the next part *Implementation.* The next phase is the confirmation of the equality of Alice and Bob's reconciled keys. And if Cascade ends successfully then the next phase will confirm the result.

5. *Confirmation*
   In order to make sure that no error will be found, Alice and Bob will exchange and compare the parity of random subsets of positions. In general, if a z parity bits comparison is done and there is no differences, then the current shared key is identical to the rate of 2^{-z}. And if this phase is successful, we probably believe that the share key is now the same, maybe with error but at an acceptable rate if z is large enough.

6. *Privacy Amplification*
   Finally Alice and Bob may have an identical key, but what about Eve? After all the previous phases, maybe she has gained some information, so it does not secure the identical shared key. So what has to be done to resolve this problem? And Privacy Amplification is exactly the answer. The aim of this phase is to minimize as far as possible Eve's information about the key and to generate a shorter but more confident key. At that moment, Eve collects only a negligible amount of information about this string and Alice and Bob can safely use it directly for unconditionally secure encryption. For privacy amplification, a publicly known universal hash functions is always chosen, that will map n-bit strings to r-bit strings. This choice can be determined over the public channel. And this proposition was made by Charles Benett, Gilles Brassard, Claude Crepeau, and Ueli Maurer.

3.3.2 Security of BB84

As we know, normally, a protocol is said to be secure when it is proved to be secure against all attack strategies of eavesdropping. This is called *unconditional security*, i.e. without assumptions. And up to now, this is still really difficult duty even for an idealized system such as BB84 protocol with single-photon source.

Proof of BB84'security

The security of BB84, however, has been theoretically proved by different scientists. In this section, some proofs will be given to readers but only as overview. For more details, refer to listed documents.

Mayers' proof [16]
The first one should be mentioned here is the Dominic Mayers'proof in 1996, more than a decade since the original proposal of BB84, which is general but rather complex one. D. Mayers followed some other previous proofs by Eli Biham or collaborators and Michael Ben-Or. To prove the BB84's security, positive operator valued measure (POVM) was applied. In his proof, he used basic techniques, the proof of security of a practical quantum key distribution protocol against all attacks allowed by quantum mechanics.

Lo and Chau's proof [34]
Quantum key distribution is widely thought to offer unconditional security in communication between two users. Unfortunately, a widely accepted proof of its security in the presence of source, device and channel noises has been missing. This long-standing problem is solved in this proof showing that, given fault-tolerant quantum computers, quantum key distribution over an arbitrarily long distance of a realistic noisy channel can be made unconditionally secure. The proof is reduced from a noisy quantum scheme to a noiseless quantum scheme and then from a noiseless quantum scheme to a noiseless classical scheme, which can then be tackled by classical probability theory.

Peter W.Shor and John Preskill's one [41]
Shor and Preskill have brought us a simple proof of security of the BB84 protocol. They used Entanglement Distillation Protocols (EDP) to prove security of BB84. Firstly, a key distribution protocol based on entanglement purification is constructed and can be proven secure using methods from Lo and Chau's proof of security for a similar protocol. And then the security of this protocol is shown to imply the security of BB84. The EDP uses Calderbank-Shor-Steane (CSS) codes, and properties of these codes are used to remove the use of quantum computation from the Lo and Chau protocol.

Daniel Gottesman and Hoi-Kwong Lo's proof [14]
To prove the security of BB84, against the most general attack, like Shor-Preskill, Gottesman and Lo use the entanglement purification except in two ways. They prove clearly the advantage of classical post-processing with two-way classical communications over classical post-processing with only one-way classical communication in QKD. This is done by the explicit construction of a new protocol for (the error correction/detection and privacy amplification of) BB84 that can tolerate a bit error rate of up to 18.9%, which is higher than any BB84 scheme with only one-way classical communications can possibly tolerate (normally 11%[23]). So their protocol leads to a higher key generation rate and remains secure over longer distances than previous ones. And moreover, their investigation suggests that two-way entanglement purification is a useful tool in the study of advantage distillation, error correction, and privacy amplification protocols.

Despite all of above proofs, BB84 still remains unsecured due to lack of authentication. Once Eve acts as inter-mediator which means that Eve acts as Alice with Bob and inversely as Bob in communication with Alice and that leads the loss of BB84's security. It is the *man-in-the-middle* attack. A solution will be proposed in the sub-section 3.3.2 on page 37. Moreover, another challenge for the assurance of security of BB84 is the source of photon. When each pulse contains more than one photon, Eve can use indirect-copy to attack BB84. She could extract only one in the transmitted beam of photons. Nevertheless, this issue has been being researched by physicists to create an apparatus generating one photon each pulse.

 © Eurocontrol, June 2004.

Considerable parameters

In the implementation of BB84, many parameters have to be taken into account. In this part, some of the most major ones will be examined. And all the information was referred and extracted from the article [10], the report of the first implementation of BB84 and a software developed for driving the quantum cryptography experiment [1].

These parameters will be divided by the concerning actors. Thus, they fall into four portions: general quantum parameters, Alice's ones, Bob's ones and Eve's ones.

- **Quantum's parameters** These ones are related to the quantum channel. In fact, a real quantum channel causes noises itself because of the imperfection of channel's material. So to have a successful simulation of a quantum channel, the factor of quantum channel efficiency should be added (called for short as Q_{eff}). And this one will be later on included into the capacity of detecting photons at Eve's and Bob's detector. Besides, the intensity of photons transmitted in quantum channel is considerable. Because in fact, it has not been possible yet to transmit a single photon each time, so in the realized experiment, they had to replace single photon by faint pulses which contain few photons. That is why the intensity of the beam (λ) is included as a parameter of quantum channel.

- **Alice's parameters** Almost considered factors will be found in Alice's configuration. The first one is mentioned here is the raw transmission size ($RawKey_{len}$), the length of Alice's initial string of qubits to send.

  After Base Announcement, the plain key (sized $PlainKey_{len}$) is achieved. A proportion of this key (EE_{sample}) will be randomly taken as a sample for Error Estimation. And then error-rate (err_{rate}) will be estimated as following:

  $$err_{rate} = \frac{EE_{sample}}{PlainKey_{len}}$$

  In the next phase, Reconciliation, Cascade, an interactive and parity-based error-correction scheme, are repeated several times. Before running this protocol, the initial block size (blk_0) for parity testing must be chosen together with the number of rounds.

  The initial block size blk_0 is chosen to be:

  $$blk_0 = \frac{1}{err_{rate} + \frac{1}{4\ err_{rate}}}$$

  The block size blk_{i+1} is defined as blk_{i+1} = 2*blk_i The last normal round occurs when the block size exceeds $\frac{1}{4}$th of all bits. Two extra passes are used with block size about $\frac{n}{4}$. Note that block size never exceed $\frac{1}{4}$th of all bits.

  In this phase named Error Correction in [10], there is another choice of these parameters. As in that implementation, the block size is chosen experimentally in turn to be 5, 7, 10, 14.

  And the size for Confirmation sample is 15 as mentioned in [10]. Due to the security analysis in [1], the value for the extra-shrinking parameter,

another name as security parameter, in privacy amplification is selected as below:

$$s = PA_{para} * (PlainKey_{len} - EE_{sample})$$

- **Bob's parameters** Bob's parameters are in relation with his detector. In fact, a detector, as the quantum channel itself, has its own efficiency which represents its capacity to detect successfully a photon. This is called for short as D_{eff}. Another problem affecting Bob's received bits rate is dark count. When the detector takes a detection event (detector's click) without any photon, dark count is generated. So dark count rate is also included in the detector capacity and cite as dc_{rate}.

- **Eve's parameters** Eve's attack capacity is dependent on these parameters. For beam-splitting attack, there are two parameters to be configured. One is the proportion of total pulses to attempt to split (*BS*), and the other is the proportion of beam (number of photons in a pulse) desired to split (*Mirror-Strength*). In applying Intercept-Resend, the first factor to be considered is proportion of beams to intercept (*IR*) and the second is about the intensity of resent beam ($Resend_{intensity}$).

- **Formulas used in this protocol**(referred to [10]) These formulas are divided into two portions. One concerns Eve's info, the others about the info in quantum channel.

  - *Estimation of Eve's info*
    In Privacy Amplification, function $h(x)$ from the class of hash functions $0,1^n \rightarrow 0,1^{n-l-s}$ (of which n is $PlainKey_{len}$, l is EE_{sample}, and s is arbitrary security parameter) is selected. It is estimated that Eve knows at most l deterministic bits before this phase. And then, Eve's amount of info is recalculated as below:

$$m = \frac{2^{-s}}{\ln 2} \tag{3.1}$$

    The number of bits leaked to Eve is estimated by simply calculating the sum of number of bits received by Eve by both beam-splitting and intercept/resend. The equation 3.2 gives the rate of bits leaked to Eve by intercept/resend with p - error rate in the channel, referred as err_{rate} in Alice's parameters:

$$IR_{rate} = \frac{4}{\sqrt{2}}p \tag{3.2}$$

    And in attack by beam-splitting, it is assumed that every pulses, at intensity of μ, will be beam-splitted with successful rate of 100% for safety. So that Eve can learn a portion of μ bits through beam-splitting. The total rate of bits leaked to Eve by two types of attacks is estimated by equation 3.3:

$$BS_{rate} = \mu Eve_{bitrate} = \rho = \mu + \frac{4}{\sqrt{2}}p \tag{3.3}$$

    In order to take into account all sampling errors we have encountered in the estimations above, it should be added on the Eve's expected key size a number of standard deviations. And this additional

 © Eurocontrol, June 2004.

part can be computed as in 3.4 where N is the length of confirmed key.

$$\sqrt{N(\mu(\mu-1)+(4+2\sqrt{2})p)} \tag{3.4}$$

Now we can get the estimated length of Eve's key by simply multiplying the number of bits in the confirmed key by Eve's bit rate with additional part of standard deviation. And finally, Eve's assumed key size is the result of 3.5:

$$Eve_{keysize} = N\rho + 5\sqrt{N(\mu(\mu-1)+(4+2\sqrt{2})p)} \tag{3.5}$$

– *Quantum Channel Simulation*
To successfully simulate the quantum key exchange, it is necessary to pay an adequate attention to quantum channel.
The crucial aspect of a quantum channel is in which a photon is subject to Heisenberg's Uncertainty Principle. As mentioned in 3.2.1 on page 26, uncertainty principle simply states that it is incapable to observe something without affecting it. And to simulate this, Quantum Channel object just does not allow Bob and Eve to access directly to buffer but rather make them use the methods which decide if Eve's and Bob's measurements are correct or not, and update data in buffer before returning a result.
Another aspect concerns the simulation of transmitted pulses of light rather than single photons in the channel. In this simulation, this is resolved by using Poisson distribution about intensity of photons μ to decide whether at least one photon exists in that pulse or not. It operates simply like this: after Alice sends a pulse to Bob in such a way as to produce an average of μ photons, this pulse reaches to Eve's or Bob's detector, quantum channel invokes the PhotonExist method of Poisson class and the result returned is either true or false. And below, one can find the formula 3.6 used to calculate the probability of x occurrences in Poisson distribution about a mean of μ.

$$f(x) = \frac{\mu^x.e^{-\mu}}{x!} \tag{3.6}$$

The following equation 3.7 returns the probability of at least one occurrence in the same distribution:

$$P(x \geq 1) = 1 - p(0) = 1 - \frac{\mu^0.e^{-\mu}}{0!} = 1 - e^{-\mu} \tag{3.7}$$

This formula is used in the method $PhotonExist$ being called each time Eve or Bob detect a photon. In $BeamSplitting$, bigger portion of a pulse will be splitted by Eve, with higher probability that Eve detects a photon.

Some types of Attacks of Eve against BB84

During the communication between Alice and Bob, Eve can be trying to listen both quantum and classical channel. She can, we assume, easily pick up everything that travels over the insecure channel (classical one). And for the quantum channel, Eve applies some following typical attack strategies to dig as maximum information as possible.

Intercept-Resend

Intercept-resend is the most used strategy which Eve applies to attack BB84. This simple and even practical attack consists for Eve to measure each qubit in one of the two bases, precisely as Bob does. Then she prepares a qubit in a state corresponding to her measurement result. She sends this qubit to Bob. Eve has a probability of 50% to correctly measure the qubit sent by Alice. In this case, she can resend successfully the original qubit to Bob without Alice and Bob's awareness. For the other 50%, Eve causes the uncorrelation between Alice and Bob's results. That will help Alice and Bob to discover Eve's presence. In brief, the intercept-resend brings to Eve 50% information while it increases the error rate in Alice and Bob's sifted key, up to about 25% even after discarding bits measured in incompatible states. Eve normally does not apply this attack to 100% communication, just only to a fraction, say 20%, then the error rate will be only $\approx 5\%$, while Eve's achieved info up to $\approx 10\%$.

Beam-splitting [4]

The second frequently used attack is beam-splitting. Eve takes advantage of the imperfection of the system to extract the information. This is due to pulses generating not only one photon but two or more than one. And thanks to these photons in excess, Eve uses the form of half-silver mirror to split the beam of photons. Then she keeps one or two photons to measure and lets the others travel onto Bob. In this case, it is difficult to detect Eve's presence. Because splitting some photons from a beam of multi-photon will not affect the polarization of this beam. Nevertheless, Alice and Bob can pre-compromise the time delay of photon to discover Eve's appearance.

Man-in-the-middle

An evident shortcoming of BB84 is lack of authentication. Additionally, with high-level technology, Eve may think of an attack called man-in-the-middle or middleman attack, in which Eve becomes an fake. She will intercept the secure channel (quantum one) and acts as Bob with Alice and inversely. By doing so, she can achieve all exchanged information between Alice and Bob without they can notice anything. Thus, in order to break down this kind of attack, authentication is the most great concern for BB84 protocol.

Protections against attacks

We will give the most simple way to protect BB84 from the first two strategies Intercept-Resend, Beam-splitting and for the third one Man-in-the-middle, a new proposal for BB84's authentication will be produced.

The initial idea proposed by Bennett and Brassard is that if any errors were found in the raw quantum key, the key would be negotiated and also could be left off. However, this work has led to the procedure called *Privacy Amplification* that we consider as one of the main phases in BB84. In this phase, it is assumed that Alice and Bob share a secret key of length k and a set of these bits, sized s, were leaked to Eve ($s < k$). Alice and Bob estimate what amount of the key Eve possessing from intercept/resend or beam-splitting attack. Then they apply privacy amplification to make Eve's data useless. This phase is based on a hashing function in form: $0,1^k \rightarrow 0,1^{k-s-p}$, where $p > 0$ is some security parameter, to shorten the shared key in order to comb out

 © Eurocontrol, June 2004.

or minimize Eve's information. Finally, Eve can know nothing or a negligible amount of the final key between Alice and Bob.

Proposal for BB84's authentication

The original BB84 paper [9] mentioned the authentication problem and introduced a solution to it, by Wegman and Carter, based on some classes of hash functions. This solution requires a pre-shared secret small key, which is used to choose a hash function from the class to produce an authentication hash of the public correspondence between them. By the nature of universal hashing, without knowing the key, the probability to deceive the correspondence is extremely low, even with unlimited computational power.

And now we will introduce here a new authentication scheme for QKD, proposed by Dang Minh Dung, which will be added into the next section 3.3.3. For other aspects such as proof of security, you may refer to this article [36]. This authentication is based on BB84 protocol. According the author, the scheme could be applied to some other protocols equivalent to BB84: Bennett's 2 states, Bell's inequality based protocol of Ekert and so on.

Authentication scheme for QKD.

1. Alice generates a random bit string and, for presenting each bit, uses a quantum eigen state in a random basis $\oplus$, $\otimes$. Alice sends these quantum states to Bob.
2. Bob uses a random basis to measure each received quantum states.
3. Bob uses a bit string b_b to present his bases: 0 for $\oplus$; 1 for $\otimes$, encrypts this string with the prepositioned key k_b, and sends it to Alice ($b_b \oplus k_b$) using the classical channel.
4. Alice uses a bit string b_a to present her bases, and sends her used bases encrypted with the key k_a to Bob, i.e.($b_a \oplus k_a$) on the classical channel.
5. Alice and Bob decrypt the bases used by each other and could then find out ($b_a \oplus b_b$). They discard the results at all positions i with b_a[i] $\oplus$ b_b[i] = 1 and interpret the rest of results to two string x_a and x_b.
6. Alice and Bob can compare some distilled bits from x_a and x_b to detect the presence of Eve or to validate the authentication.

3.3.3 Specification for a simple implementation of BB84

In this section, a detail specification will be introduced for a simulation of QKD using BB84 protocol.

Objectives

This simulation is firstly aiming at illustrating the oldest and the most typical protocol in QKD. Secondly, it provides a rather entirely detailed specification to be easily implemented by anyone who is interested in QKD and has intention to possess his own simulation of a quantum key distribution system. Thirdly and also lastly, this implementation would experiment the proposed

authentication scheme in 3.3.2 on the preceding page. The simulation will simulate the key exchange process between two major actors Alice, Bob and an unexpected one, the eavesdropper called Eve. The exchange is realized over two channels: a quantum and a classical channel, which are considered as two others actors of system.

System requirements

For the simplicity of experimentation, the simulation will run on only one machine. The software is developed under Solaris version 8. The program will be implemented in Java, a familiar programming language with great support of graphical interfaces implementation. As Java is used, the software will be executable on almost all systems and computers.

Functions descriptions

The primary target of the simulation, as mentioned above in part *Objectives*, is to illustrate the operation of quantum cryptography in reality. In addition, it will simulate the actions of Alice, Bob, Eve and the channel between them.

Alice
Alice is the sender of the encrypted message. She must communicate with Bob to produce a random key. This will be done by following sequentially all steps in the part 3.3.1 on page 29. In other words, Alice will interact with Bob through the quantum channel in order to exchange the key. She has to prepare this key under the form of a string of random qubits. She must inform Bob about the start and end of both the message and each pulse. She is also capable of listening the channel to know when Bob finishes his detection of a pulse. Once all of the qubits have been sent and received, Alice will communicate to Bob in which bases she used to measure pulses, error correction and privacy amplification. Her communication with Bob is on both quantum and public channel. So she will interact directly with the channel object simulating her transmission of pulses in a random polarization. The final task of Alice is to display all the results of her consecutive actions for the aim of the demonstration. And she must also provide to the users an interface to modify parameters affecting the protocol such as the number of photons in a pulse or the size desired for error estimation, etc.

Bob
Bob is Alice's partner in this protocol. He is the destination of her message. Some of his functions are the same with hers like listening to channel, reading/writing the information in/to the channel. He also interacts with Eve to make as real as possible a quantum key exchange. To reply to Alice's pulse, he must acknowledge the receipt. The phase *Bases Announcement* differentiates his operation from hers. This is the broadcast of all randomly chosen bases used by his photon-detector to measure Alice's pulses. Another difference between Alice and Bob is the decision of polarization of photon. On Alice'side, this is decided by her apparatus but on Bob's side, it is done by him. But the common point here is that both choices are random. Finally, Bob must output his result in the same way as Alice's except fewer parameters to configure such as efficiency of his detector.

Eve
Eve stands in the middle of Alice and Bob. She acts both their roles at the same time. Thus, she shares with them many common functions in order to exploit

 © Eurocontrol, June 2004.

BB84. Her major motivation is to collect as much as possible the information about the shared key between Alice and Bob without being discovered. Her advantage is to be able to both receive and send pulses over the quantum channel in use (intercept/resend strategy) and to realize beam-splitting attacks. But this is limited by the configuration of channel. Lastly, her same responsibility as Alice and Bob is to lay out her actions and results as well. She must also allow users to change her configuration like percentage of intercepted message.

Channel
The objective of the simulation is to make the object *Channel* mostly like the quantum channel in reality. It means that this one must have all the properties, here the law of physics mentioned in 3.2.1 on page 26, that a real one gets. When the channel is active, it must carry the information of a pulse (number of photons in this pulse, polarization of photon in secret) from Alice/Eve to Eve/Bob, and must produce the result to their detectors measurement. The channel sometimes causes errors to the communication such as loss of pulses on transmission. And like all three actors above, the channel shows out its operations and accepts users'modification through the GUI.

Detailed Implementation

Now, we are going into the main part of this section. This is the implementation of a BB84 QKD protocol. The protocol is applied by three main characters: Alice (sender), Bob (receiver) and Eve (eavesdropper). All their communications are carried out in two separate channels: quantum (obeying quantum physics laws) and public one (using the normal laws of public communication). In using Java to develop the program, three actors will be represented by three separate threads and interact to each other by accessing into two channels implemented by two public objects. These two objects are created and observed by the Main thread. So in total, there are four threads which run simultaneously on a same computer, same Java virtual machine.

In this communication, Alice keeps the active role and Bob the passive one except his choice of the measurements polarizations and their announcement to Alice. For her part, Eve always tries her best to extract useful informations about the key from Alice and Bob's info exchange, by applying different attack methods. And for simulation of synchronicity in three person's communication, all written data into channel will be hold in a buffer. The quantum buffer can be accessed and written into by anyone. But for the public one, it is only available for everyone to read from it. But only Alice and Bob can write into it, not Eve. The moment one can access to channel for information will be decided by two objects channel. If it is the unavailable moment, the actor will receive a null value and will fall again into the wait state. In this simulation, the digit 1 will represent diagonal polarization and the digit 0 rectilinear one.

Outline class structure

As mentioned above, all transactions between three main actors: Alice, Bob and Eve are processed on both channels, firstly on quantum one, then on public one. So we will divide the following analysis of implementation into two major parts (quantum channel and public one) and a supplement one (GUI).

Quantum channel

The quantum channel is simulated as an object in the `main()` thread. It is intrinsically a controller of the string of pulses transmitted from Alice, via

Eve, to Bob. Here these pulses are implemented as qubit objects. A qubit object contains the value of correlated binary bit (0 or 1), its polarization valued 0 or 1 too, a tag field to check the interception of Eve and another for the number of photons in that pulse.

This simulated quantum channel operates as a real one in physical aspect. It provides different methods for Alice, Eve and Bob that they can interact together. They can send or read information from the channel or launch an attack upon it (for Eve). Below we have specific rules to follow:

- *Alice.* She can transmit as many qubits as she likes in her time slot without worrying about Eve or Bob's receipt yet.
- *Eve.* She cannot directly extract information from a photon, such as its polarization. She may change the polarization of a photon due to her wrong measurement. After Eve intercepts a pulse, the tag field will be changed to permit Bob's access to it.
- *Bob.* He cannot access directly to the photon to get the information of a qubit, neither read the qubit before Eve before switch of tag field.

Below is the description of qubit object:

Qubit	
`int`	`value`
`int`	`polarization`
`int`	`tag`
`float`	`photons`

Public channel

All phases of the qubit string treatment from which to distill the final key take place on public channel. Each phase is negotiated between Alice and Bob with transmitted necessary parameters. And these exchanges are repeated and have the same structure of the name phase and its parameters. So all these phases' information are fixed in the following format:

```
NamePhase:parameters - the parameters separated by ':'
```

Besides these above commands, there are two others commands New and End used by Alice to signal Bob the start and the end of a session of QKD. The simulation will be triggered by Alice's `New` command sent through public channel accompanied with the length of qubit string to be sent. Then Alice begins to send sequentially her message, one bit by one bit. This is done by using the method `Write()` of quantum channel object in producing her intended polarization, the value of this qubit, number of photons in the pulse and the order of the qubit. And this info will be written into Quantum buffer and signaled to Eve by Quantum Channel.

Alice's method `Write()` on the quantum channel

```
Write(  int Polarization,
        int value,
        float Intensity,
        int BufferLocation)
```

 © Eurocontrol, June 2004.

Eve receives the signal, from Quantum Channel, of the bits written in Quantum buffer and must at least acknowledge them before Bob is allowed to view them. This is to resolve the problem of synchronism in reality. Once Alice has transmitted all of the bits in her message, she waits for Bob's response.

When receiving a qubit, Eve chooses which attacks to be taken to read its info or let it proceed to Bob. She has different choices: beam-splitting, intercept/resend, both attacks or nothing. Eve can apply some attacks separately on the same location in quantum channel buffer. If she attempts to split the photon, she must specify both its position, and the capacity of her splitting mirror. This strength of 0 means that Eve ignores this photon and pass it to Bob while the value of 1 shows that Eve detects all the photon in the pulse and consequently, this pulse is entirely changed. In the case of a success of Eve beam-splitting, Eve knows the Alice's polarization which is saved in the buffer.

Eve's method `BeamSplitting()` on the quantum channel

```
BeamSplitting(float MirrorStrength, int BufferLocation)
```

She can also use intercept/resend attack independently. She can do this with command `IR` in provide the position of pulse, the polarization to measure photon and also value for resend strength. And the rest of the work is for the quantum channel object. It is responsible for checking the polarization chosen by Eve, to update the buffer location and to return result of the measure to Eve.

Eve's method `IR()` on the quantum channel:

```
IR(  int Polarization,
     float ResendIntensity,
     int BufferLocation)
```

Once Eve finishes her job, she must acknowledge the value and shift the flag of Bob's permission. This is accomplished by below method.

Eve's method `tag()` on the quantum channel:

```
tag(int BufferLocation)
```

After shifted bit of Bob's permission, he can read info of this photon with the same method as Eve's `IR` except without parameter `ResendIntensity`. This method will return to Bob the value of this photon or an empty message. Bob's `read()` includes the effects of noise in channel, Bob's detector efficiency and dark counts as well. All these are only applied to Bob whose technology is realistic while Eve is assumed to have a perfect technology to detect pulses.

When all bits received, Bob steps in phase Bases Announcement, sends ReceivingBase command to Alice with his sequence of pairs containing position of qubit and its guessed polarization. Bob can send to Alice a message like this:

```
ChosenBases:pos1:polar1:pos2:polar2...
```

Then, the diagonal and rectilinear polarizations are represented by digits 1s or 0s. When this message reaches Alice, she prepares a BaseConfirm message to reply to Bob in the same form of his ChosenBases except her parameters

being subset of his. Her pair contains positions where Bob measured correctly and its original polarization.

```
BaseConfirm:posi:ori.polari:posj:polarj...
```

Eve may extract useful info for her from both above messages. And she will insert a blank in her key string where she did not detect successfully or guessed correctly a photon.

In case of applying the Authentication scheme, these two messages are encrypted with two reconciled key between Alice and Bob. These messages become incomprehensible for Eve. As an expected result, the exchanged information is confidential and safe from Eve. Hence, Eve acquires no useful information from the phase BaseAnnouncement with new Authentication scheme.

Error Correcting

Error Estimation: As mentioned in part 3.3.1 on page 29, this phase is to improve the result of the next one, Reconciliation. Alice sends to Bob command ErrorEstimation with the size K of subset extracted from plain key and a sequence of pairs (position, value). And Bob returns his bits received at those positions with same command.

```
ErrorEstimation:K:pos1:value1:...:posk:valuek
```

```
ErrorEstimation:value1:...:valuek
```

Then both of them compute the observed error-rate by $\frac{ircorrelatedbits}{K}$. They reject quantum transmission in case of error-rate less than the initially set one, otherwise K bits being removed from the plain key and step to the next.

Reconciliation: This phase is for error correction. Up to now, Alice and Bob share a sequence of bits and Eve may know a part of it (without use of authentication scheme). In this common string, there may be errors caused by attacks of Eve, by noise of the quantum channel or dark counts, inefficiency of Bob's detector and etc... Reconciliation helps Bob and Alice to check and correct these errors. Alice first calculates the size of block to be used, based on the error-rate (like in 3.3.2). Then Alice divides her string into blocks of length k. And she sends all positions in each block, one block at a time, to Bob with command ErrorCheck.

```
ErrorCheck:pos1:...:posk
```

And it is Bob who calculates the parity of each block and replies to Alice this parity with command ParityConfirm.

```
ParityConfirm:parityBlocki
```

Then Alice and Bob both delete the last bit of block to avoid info leakage to Eve.

Alice compares her parity with the one sent from Bob. If they match then this block is considered correct. Otherwise, Alice uses bisective searches to find and remove errors. They repeat this work through all blocks sized k and also with $2^n k$ until block size over-passes $\frac{1}{4}$ of plainkey's length.

Confirmation: To eliminate maximum errors from shared key, Alice continues her work with subset of randomly picked positions rather than a continu-

 © Eurocontrol, June 2004.

ous block.

Privacy Amplification: Now, Alice and Bob may be sure that their shared key has no errors or a negligible quantity but it is partially secured only. So they have to carry out the Privacy Amplification. This phase is performed by a simple round of random subset hashing. To this extent, Alice declares sets of bits with PrivacyAmplification command. Then Alice and Bob both calculate the parity bit of the random subset. But they do not reveal their result. And this result makes out the final key !

Finally, Alice sends End command to Bob through public channel to inform him about the termination of the QKD.

The GUI
For graphical part, the package Swing of javax will be exploited. Each object in this simulation has its own graphical interface. These GUI are extended from JFrame. For three actors, these interfaces are implemented in separate frames within three corresponding classes: AliceInt.class, EveInt.class and BobInt.class. Each interface contains a tab for setting, another for result or both. In the tab for setting, text fields (correspond with their parameters) are included to allow users to enter desired values to experiment. The one of Alice has a little more difference in having additional button *Start* used to initiate the protocol.

Two other ones are for quantum channel and public one. Both of these are included in QuantumChannel class and PublicChannel class.

And below is the description of principal parameters to be configured, before the start of simulation, in each interface of actors and also the two channels. (further details, referred to 3.3.2)

- Alice's setting
  - *Transmission Size* is an integer larger than 0 and less than 1000000 (because the buffer location is limited by 1000000). This is the size of qubit string transmitted on the quantum channel.
  - *Beam Intensity* is a floating point number in the interval [0, 1]. This number decides Eve or Bob's successful rate when detecting a photon. And it is also the proportion of bits assumed to be successfully detected by Eve in use of beam-splitting.
  - *Confirmation Sample Size* is the number of bits chosen randomly in phase Confirmation. It is an integer greater than 0.
  - *Security Factor* is an integer, added to Eve's assumed key size before privacy amplification. It allows to increase the security of the system by an additional factor.
- Eve's setting
  - *Beam Split* is a floating point number between 0 and 1. This is the percentage which Eve takes for beam splitting.
  - *Mirror Strength* is floating point number 0 to 1 inclusive. This is used to decide how much of a pulse is used for beam-splitting.
  - *Intercept/Resend* This is similar to Beam Split but used for Intercept.

  - *Resend Strength* After intercept a pulse from Alice, Eve does not know the intensity. So she must create her own pulse with a new intensity.

- Bob's setting In Bob's interface, there is only one result box which display the key bits and its length through each phase.
- Quantum channel's setting
  - *Mirror Efficiency* its value is in the interval [0,1]. When Eve takes action of splitting a pulse, it absorbs partially this photon. So lower mirror efficiency means much more photons absorbed from the pulse.
  - *Channel Efficiency* is to measure channel's interference to the pulse upon it. Higher this rate is, less interference on pulses.
  - *Detector Efficiency* measures the capability of Bob's detector. Its value is in $[0, 1]$.
  - *Dark Counts* represents the sudden occurrence of a dark count at Bob's detector.
- Public channel's setting This interface has only one tab: the result to display the current transmission upon it and each passed phase's result.

Relation of all objects implemented in this simulation is described in below graph 3.3.3

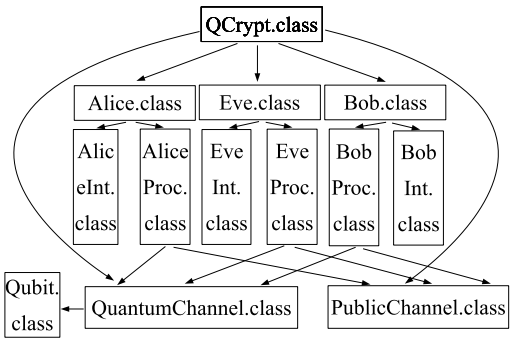


Figure 3.3: Diagram of relation among principal objects in simulation of BB84 protocol

There are in total five principal classes: two channel objects and three actors in this communication. All three actor objects have the same structure. They all implement the Runnable interface which allows to be launched as three separate threads by Qcrypt class. Each of the actors has two other classes: an Interface class and a Protocol class.

The Interface classes are described as in the part just above, *The GUI*.

And Protocol ones are instantiated by the major classes Alice class, Eve class and Bob class when button start in Alice's interface is clicked. They begin by setting up all parameters with the values got from the Frame object and activate their RunProtocol() method. This method helps actors to go through all phases of BB84 protocol and displays the correlated result with each phase to the correspondent interface.

 © Eurocontrol, June 2004.

Section 4

Free Space and Satellites

The development of physical techniques plays an important role in the growth of practical applications of *Quantum Cryptography* (QC). As you know, one QC system contains at least one transmitter (photon source), one receiver (detector) and one quantum channel. Fiber-based links is one of two solutions for quantum channel, the other is free-space links. Most of research so far use optical fibers to guide the photons from Alice to Bob. Although today's fiber-based QC systems are very advanced, such systems cannot work over the distance of 150km [30] due to the combination of fiber losses and detector noise, moreover, fiber-based links may not always be available due to some other reasons. Hence, there are more and more efforts in developing free-space links, where the photons are sent between remote telescopes.

The very first demonstration of free-space QC system was a table-top experiment performed at the IBM Thomas J.Watson Research Center in 1989 over a distance of 32cm [5]. With the progress of technology, the most recent result of a such system has achieved a distance of 23.4km [31]. And the theoretical calculations allow us to hope a free-space communication up to 1600 km, suitable for satellite-based key exchange. In this section, we will see the state of the art of free-space QC systems, also, the overview of satellite communications and networks for the estimation of possibility to apply QC in satellites for the global key distribution, which is the ultimate goal of such systems.

4.1 Free Space

Free-space links have been studied and already successfully implemented for several years for their application in quantum cryptography based on faint classical laser pulses [7, 8, 20, 26, 31]. Free-space link is one of two solutions for quantum channel. Transmission over free-space links has some advantages compared to the use of fiber-based links. First of all, the atmosphere has a high transmission window at a wavelength of around 800 nm, where photons can easily be detected using commercial, high-efficiency photon detector. Furthermore, the atmosphere is only weakly dispersive and essentially isotropic at these wavelengths. It will thus not alter the polarization state of a photon.

However, there are some drawbacks concerning free-space links as well. In

© Eurocontrol, June 2004.

contrast to the signal transmitted in a optical fiber (guiding medium) where the energy is protected and remains localized in a small space, the energy transmitted via a free-space link spreads out, leading to higher and varying transmission losses. In addition, the background light such as ambient daylight or even moonlight at night can couple into the receiver, leading to dark-count errors. Finally, it is clear that the performance of free-space QC systems depends dramatically on atmospheric conditions.

4.1.1 State of the art

The idea of QC was first proposed in the 1970s by Stephen Wiesner and by H.Bennett of IBM and G.Brassard of The University of Montréal. However, this idea is so simple that any first-year student since the infancy of quantum mechanics could actually have discovered it. Nevertheless, it is only now that the QC theory is mature enough and information security important enough that physicists are ready to consider quantum mechanics, not only as a strange theory good for paradoxes, but also as a tool for new engineering.

The first protocol for QC was proposed in 1984 by H.Bennett and G.Brassard, hence the name BB84. After this, the other more effective was born such as two-state protocol, six-state protocol, Einstein-Podolsky-Rosen protocol and so on. But most of QC experiments so far are limited on BB84 by its simplicity and the limitation of physical devices.

One of the most important of QC systems is the choice of photon sources and photon counters. Optical quantum cryptography is based on the use of single-photon Fock states. Unfortunately, these states are difficult to realize experimentally. Nowadays, practical implementations rely on faint laser pulses or entangled photon pairs, in which both the photon and the photon-pair number distribution obey Poisson statistics. For large losses in the quantum channel, even small fractions of these multi-photons can have important consequences on the security of the key, leading to interest in “photon guns”. As for the photon counter, in principle, this can be achieved using a variety of techniques, for instance, photon-multipliers, avalanche photo-diodes, multi-channel plates, and super-conducting Josephson junctions [19].

Today, the best choice of wavelength for free-space QC systems is of 800 nm for which efficient *avalanche photo-diodes* (APD) counters are commercially available. In addition, the receiver uses a combination of spectral filtering, spatial filtering and timing discrimination using coincidence window of typically a few nanoseconds to decrease the dark-count errors. Free-space transmission is restricted to line-of-sight links. Thus, the beam-pointing is still difficult for moving targets.

Despite the progress of the QC theory, the free-space QC systems are not popular. In the early 1990s, the first experiment performed by Bennett and co-workers at the IBM laboratory over a distance of 30cm [5]. After this, there are some others significant free-space experiments:

- 1996 J. Franson, Baltimore : 150 m, daylight
- 1998 R. Hughes, Los Alamos : $\sim$1 km, night [7]
- 2000 R. Hughes, Los Alamos : 1.6 km, daylight [8]

 © Eurocontrol, June 2004.

- 2001 J. Rarity, QinetiQ : 1.9 km, night [20]
- 2002 R. Hughes, Los Alamos : over 10 km [26]
- 2003 P. Morris : 23.4 km, night [31]

The results achieved of P. Morris form a significant step towards a key exchange system. Such a system using slightly bigger telescopes, optimized filters and anti-reflection coasting, combined with sophisticated automatic pointing and tracking hardware, could be stable up to 34dB of loss - the limitation of loss acceptable for QC system - and capable of maximum ranges exceeding 1600km. We could engineer the possibility of the exchanged keys with low earth orbit satellites such as a secure 'relay' station this has the potential for secure key exchange between any two arbitrary locations on the globe.

For a better understanding, we will study the most recent success of free-space QC system of P. Morris.

4.1.2 The most recent success

From September 2001 to January 2002, P. Morris have tested a semi-portable free-space QC system between two mountain tops, Karwendelspitze (2244m) and Zugspitze (2960m), in Southern Germany, for the exchange of keys [31]. The distance between the two locations is 23.4km. The elevated beam path dramatically reduced the air turbulence effects experienced in previous low altitude tests, but also caused unprecedented requirements on stability against temperature changes, reliability under extreme weather conditions and ease of alignment.

The transmitter, named Alice, encodes a random binary number in weak pulses of light using one linear polarization to encode '1's and orthogonally polarized pulses to encode zeros. To prevent eavesdropping the number of photons per pulse is limited to much less than unity (the actual attenuation is linked to the overall transmission and is usually chosen as 0.1 photons per pulse). Furthermore, the encoding basis is randomly changed by introducing a 45^o polarization rotation on half the sent pulses. In the receiver, named Bob, single photon counting detectors detect the pulses, converting the light to macroscopic electronic pulses. The two polarizations are separated in a polarizing beam-splitter and a zero or one is recorded depending on the detected polarization. A random switch selects whether to measure in a 0^o or 45^o polarization basis. Due to the initial attenuation and the attenuation along the transmission line only very few of the sent pulses result in detected events at the receiver. A record of when the pulses are detected is kept and at the end of the transmission the receiver uses a classical channel (for instance the telephone line) to tell the sender which pulses arrived and what basis they were measured in. All lost pulses and all detected pulses measured in a different basis to the encoding basis are erased from the sender's record. Thus identical random keys are retained by sender and receiver. Any remaining differences (errors) signal the interception of an eavesdropper! If an eavesdropper measures the polarization of one pulse, that pulse, being a single photon, is destroyed and does not reach Bob and thus is not incorporated in the key. The eavesdropper could choose a basis, measure the pulses then re-inject copies. However, this strategy has to fail because half the time the eavesdropper will

have chosen the wrong measurement basis and the re-injected pulses will induce an error rate of 25%. Of course a certain level of error could be caused by imperfections in the equipment used, but in order to guarantee absolute security any error should be attributed to (partial) interception. Below a certain threshold the error can be corrected and potential knowledge of the key by any eavesdropper can be erased by privacy amplification protocols.

It is similar to all of QC systems, the QC system of P.Morris consists of 3 main components:

- transmitter
- detector
- quantum channel (free-space)

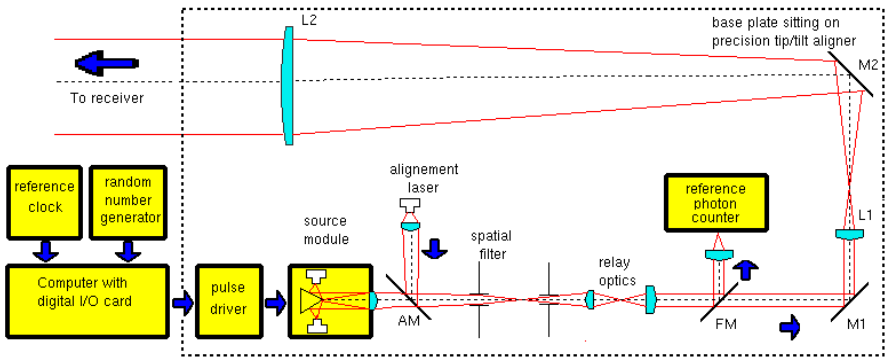


Figure 4.1: The Alice compact 20x50 cm breadboard transmitter

The transmitter (figure 4.1) is designed round a 80 mm diameter transmit telescope. The digital I/O card delivers a random 2-bit signal at 10 MHz synchronized to the reference clock. This signal is used in the pulse driver for randomly firing one of four 500 ps (picosecond) duration lasers (850 nm wavelength) in the miniature source module. This miniature source uses polarization approximating coded faint pulses in the place of single photons. The four lasers are combined in a spatial filter using a conical mirror and relay lens. Each laser is rotated to produce one of the four polarizations: 0^o, 90^o, 45^o or 135^o and illuminates a spatial filter consisting of two pinholes with a diameter of 100 μm spaced at a distance of 9 mm.

Since the overlap of the emission modes of the four laser diodes with the filter mode is rather poor, the initially very bright laser pulses are attenuated to about the required "one photon per pulse" level. This system uses pulses with 0.05-0.5 photons per pulse. The actual attenuation can be fine tuned by manipulating the diode current and precisely calibrated by optionally shining the light transmitting the spatial filter onto a single photon detector. The filter erases all spatial information about which laser diode fired. Spectral information is also not attainable by an eavesdropper, as the spectra of the four laser

 © Eurocontrol, June 2004.

diodes well overlap with a width of about 3 nm in pulsed mode. A bright *continuous wave* (CW) laser beam can be injected with an auxiliary mirror AM for alignment purposes into the same spatial filter as the faint pulses, while a calibration of the number of photons per bit can be made by inserting mirror FM and measuring a reference photo-count.

The output of the spatial filter is then transformed to a collimated beam with 2 mm *full width at half maximum* (FWHM) and further expanded in a x20 telescope (L1 and L2) to produce a near diffraction-limited 40mm FWHM beam. A precision translator with lens L1 allows the fine focus adjustment. Mirrors AM, FM, M1 and M2 are gold coated for high reflectivity in the infrared. Together with the alignment laser and the single photon detector, the whole system is mounted on a 25x50 cm breadboard, attached to a micro-radian sensitive pointing stage on a sturdy tripod. The computer uses a pre-stored random number to choose the polarization for the present set of experiments. Alternatively, nearly real time generation was possible, where a sequence of bits produced by a quantum random number generator running at 20 MHz was produced in the second right before the transmission.

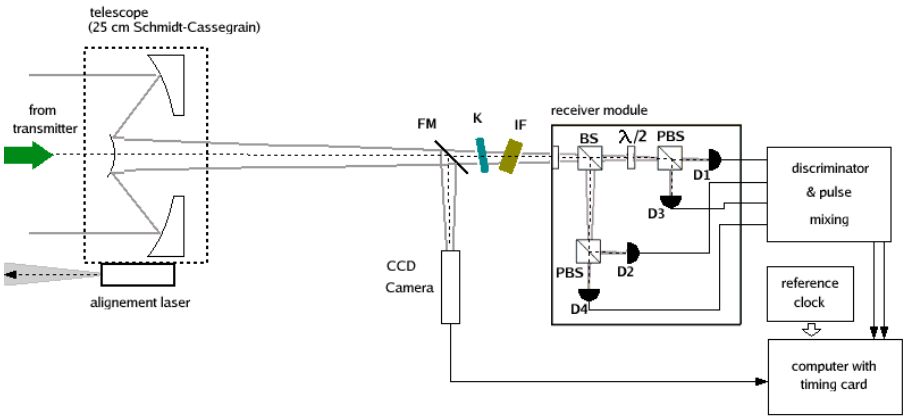


Figure 4.2: The receiver (Bob): Schmidt-Cassegrainian telescope and attached miniature detector module

The receiver system (figure 4.2) consists of a 25 cm diameter commercial telescope (Meade LX200) with computer controlled pointing capability realized by using a flip mirror and a CCD camera to view the incoming light. Unfortunately, the resolution of the mechanics of this system was the limiting factor for the alignment of the receiver, and was also difficult to handle at the harsh outdoor conditions. A compact four-detector photon counting module 12 was coupled to the back of the telescope after an RG780 long pass filter to block out short wavelength background. The module consists of a *non-polarizing beam-splitter* (BS) passing two beams to *polarizing beam-splitters* (PBS) that are followed by four photon counting avalanche diodes. One polarizing beam-splitter (in the D1/D3 arm) is preceded by a 45^o polarization rotator (half wave plate). Photons detected in this channel are thus measured in the 45^o basis, while the other polarizer allows measurement in the 0^o-90^o basis. Since the splitting of incoming photons to the two analyzers by the beam-splitter is truly random, no random number sequence nor any space consuming optics are required on the receiver side, however. The module incorporated high voltage supplies and discriminatory circuitry to produce standard NIM pulses at the output. The

detector outputs D3, D4 are combined with the D1, D2 outputs with a delay of 5 ns and input into the two channel time digitization card (Guide Technology GT654) in the PC. Thus the four detectors outputs are combined into the two channels with a delay of 5 ns. The delay is then used to discriminate between the two measurement bases. The overall optical detection efficiency of the receiver is about 16%, timing jitter was smaller 1 ns.

Beside of quantum devices, the timing and the synchronization are very important. The two separate computers were linked via modems operating over a standard mobile telephone link (9.6 Kbaud bit rate). Local oven-stabilized 10 MHz clocks were synchronized to better than l ns using a software phase locked loop driven by the received photo-detections. The photo-detections thus can be gated in two 1.4 ns wide time windows separated by 5 ns. Pulses outside these timing gates are ignored. The error rate due to dark and background counts is thus suppressed by a factor of $\sim$1/35. The random polarization pulses are sent in 700 ms blocks preceded by a series of predetermined pseudo-random data sets lasting 110 ms to uniquely determine the start time of each block. Following the transmission of the block a settling time of $\sim$300 ms allows the computers to check for a successful transmission. Gross block length is thus just over 1.1 s. Sifting and error correction of the 700 ms data blocks were then performed over the telephone link using software developed in the 1.9 km experiment [20].

Figure 4.3 shows some results achieved :

Night	Number of photons per bit (+/-10%)	unsifted data bits/s	Back-ground bits/s	Quantum bit %	Final net bits/s
16/01/02	0.37	4484	6268	4.11 (1.96)	626
16/01/02	0.27	2505	5504	5.24 (3.08)	396
16/01/02	0.18	2651	5578	4.54 (2.94)	363
16/01/02	0.096	2627	4516	4.77(2.41)	367

Figure 4.3: Summary of selected experiments

4.2 Satellites Communication

4.2.1 Overview of satellites communication

Not so long ago, satellites were exotic, top-secret devices. They were used primarily in a military capacity, for activities such as navigation and intelligence. Now they are an essential part of our daily lives. Communication satellites allow radio, television, and telephone transmissions to be sent live anywhere in the world. Before satellites, transmissions were difficult or impossible at long distances. The signals, which travel in straight lines, could not bend around the round Earth to reach a destination far away. Because satellites are in orbit, the signals can be sent instantaneously into space and then redirected to another satellite or directly to their destination.

 © Eurocontrol, June 2004.

A communication satellite functions has an overhead wireless repeater station that provides a communication link between two geographically remote sites. Due to its high altitude, satellite transmissions can cover a wide area over the surface of the earth. Each satellite normally is equipped with various "transponders" consisting of a transceiver and an antenna tuned to a certain part of the allocated spectrum. The incoming signal is amplified and then rebroadcast on a different frequency. Most satellites simply broadcast whatever they receive, and are often referred to as "bent pipes". These were traditionally used to support applications such as TV broadcasts and voice telephony. In recent times, the use of satellites in packet data transmission has been on the rise. They are typically used in WAN networks where they provide backbone links to geographically dispersed LAN's and MAN's [18].

Normally, satellite links can operate in different frequency bands and use separate carrier frequencies for the up-link and down-link. The figure 4.4 shows the most common frequency bands. The use of C bands was most common in 1st generation Satellite systems. However this band is already crowded as terrestrial microwave links also use these frequencies. The current trend is towards the higher frequencies of Ku and Ka bands. Attenuation due to rain is a major problem in both of these bands. Also due to the higher frequencies, microwave equipment is still very expensive, especially in the Ka band.

BAND	UP-LINK (GHz)	DOWN-LINK(GHz)	ISSUES
C	4 (3.7-4.2)	6 (5.925-6.425)	Interference with ground links
Ku	11(11.7-12.2)	14 (14.0-14.5)	Attenuation due to rain
Ka	20 (17.7-21.7)	30 (27.5-30.5)	High Equipment cost
L/S	1.6(1.610-1.625)	2.4(2.483-2.500)	Interference with ISM band

Figure 4.4: Frequency spectrum allocation for some common bands

The area of the earth's surface covered by a satellite's transmission beam is referred to as the "footprint" of the satellite transponders. The up-link is a highly directional, point to point link using a high gain dish antenna at the ground station. The down-link can have a large footprint providing coverage for a substantial area or a "spot- beam" can be used to focus high power on a small region thus requiring cheaper and smaller ground stations. Moreover, some satellites can dynamically redirect their beams and thus change their coverage area.

Satellites can be positioned in orbits with different heights and shapes (circular or elliptical). Based on the orbital radius, all satellites fall into one of the following three categories:

- *Low-Earth Orbit* (LEO)
- *Medium Earth Orbit* (MEO)
- *Geostationary Orbit* (GEO)

Some features of 3 satellite types are showed in the figure 4.5 on the following page.

Type	LEO	MEO	GEO
Height	100-300 miles	6000-12000 miles	22,282 miles
Time in LOS	15 min	2-4 hrs	24 hrs
Merits	Lower launch costs, very short round delays, small path loss	Moderate launch cost, small round-trip delays	Covers 42.2% of the earth's surface, constant view, no problems due to dropper
Demerits	Very short life 1-3 month, encounters radiation belts	Larger delays Greater path loss	Very large round trip delays Expensive ES due to weak signal

Figure 4.5: Salient features of different satellite constellations

Satellites are also classified in terms of their payload. Satellites that weigh in the range of 800-1000 kg fall in the "Small" class, whereas the heavier class is named as "Big" satellites. GEO satellites are typically "Big" satellites, whereas LEO satellites can fall in either class [18].

Some protocols for the satellites communication:

- ALOHA : It is one of the basic protocol in the packet radio communications. The ALOHA system has a simple structure and easy control. However, it is difficult to receive a packet correctly if packet collision occurs.
- *Frequency Division Multiple Access* (FDMA): It is the oldest and still one of the most common method for channel allocation. In this scheme the available satellite channel bandwidth is broken into frequency bands for different stations.
- *Time Division Multiple Access* (TDMA): In this method, channels are time multiplexed in a sequential fashion. Each earth station gets to transmit in several fixed time slot only.
- *Code Division Multiple Access* (CDMA): This scheme uses a hybrid of time/frequency multiplexing and is a form of spread spectrum modulation. It is a relatively new scheme but is expected to be more common in future satellites.
- *Packet Reservation Multiple Access* (PRMA): It is an improved form of TDMA that combines TDMA with the techniques of Slotted-ALOHA.

Up to now, there are various uses of satellite communication [1]:

- Traditional Telecommunications
- Cellular
- Television Signals
- Marine Communications

[1] http://www.cis.ohio-state.edu/~jain/cis788-97/satellite_nets/index.html

 © Eurocontrol, June 2004.

- Spacebourne Land Mobile
- Satellite Messaging for Commercial Jets
- Global Positioning Services

There are some modern satellite networks, for instance, IRRIDIUM, INMARSAT M, GLOBALSTAR, TELEDESIC, ODYSSEY, ICO, GPS. For a little knowledge about satellite networks, we will see the GPS that is one of the most known satellite networks.

The *Global Positioning System* (GPS) is a "constellation" of 24 well-spaced satellites that orbit the Earth and make possible for people with ground receivers to pinpoint their geographic location. The location accuracy is anywhere from 100 to 10 meters for most equipment. Accuracy can be pinpointed to within one meter with special military-approved equipment. GPS equipment is widely used in science and has now become sufficiently low-cost so that almost anyone can own a GPS receiver.

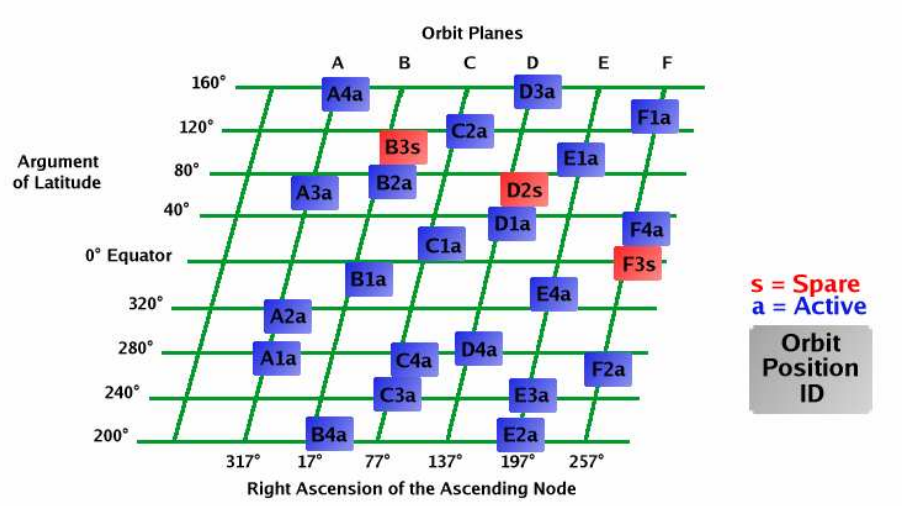


Figure 4.6: Simplified Representation of Nominal GPS Constellation

The GPS is owned and operated by the U.S. Department of Defense but is available for general use around the world. Briefly, here is how it works:

- 21 GPS satellites and three spare satellites are in orbit at 10,600 miles(20,200 km) in 6 orbital planes above the Earth. The satellites are spaced so that from any point on Earth, four satellites will be above the horizon (figure 4.6).
- Each satellite contains a computer, an atomic clock, and a radio. With an understanding of its own orbit and the clock, it continually broadcasts its changing position and time. (Once a day, each satellite checks its own sense of time and position with a ground station and makes any minor correction.)
- On the ground, any GPS receiver contains a computer that "triangulates" its own position by getting bearings from three of the four satellites. The

result is provided in the form of a geographic position - longitude and latitude - to, for most receivers, within 100 meters.

- If the receiver is also equipped with a display screen that shows a map, the position can be shown on the map.
- If a fourth satellite can be received, the receiver/computer can figure out the altitude as well as the geographic position.
- If you are moving, your receiver may also be able to calculate your speed and direction of travel and give you estimated times of arrival to specified destinations.

The GPS is being used in science to provide data that has never been available before in the quantity and degree of accuracy that the GPS makes possible. Scientists are using the GPS to measure the movement of the arctic ice sheets, the Earth's tectonic plates, and volcanic activity.

4.2.2 Satellites Free-space Communication

At present, the only suitable systems for long-distance quantum communication are photonic. Other systems such as atoms or ions are studied thoroughly, however their applicability for quantum communication schemes is presently not feasible within the near future, using photons as the only choice for long-distance quantum communication. The use of satellites to distribute photons provides a unique solution for long-distance quantum communication networks. This overcomes the principle limitations of Earth-bound technology, i.e. the narrow range of some 100 km provided by optical fiber and terrestrial free-space links. While this may not seem like much, free-space QC transmission between two ground-based locations 2km apart is equivalent to from a ground-based location to an orbiting satellite at 300km altitude. Photon sources and detectors presently implemented in such classical space laser communication systems can, in general, not be directly employed in quantum communication systems. However, the available experience may serve as a starting point for the development of space qualified components needed for quantum space experiments.

For the satellite free-space QC transmission, the main difficulty would come from beam pointing and wandering induced by turbulence because in space, atmospheric interference problems go away. Then, minimizing the size and weight of the equipment is vital as it is ever going to be installed on a satellite. The major design parameters for the transmission subsystem are laser wavelength, modulation format and data rate, and reception technique. Of equal importance is the subsystem required for beam pointing, link acquisition, and automatic mutual terminal tracking *Pointing Acquisition and Tracking QC Quantum* (PAT). Because of the very narrow widths of the communication beams involved, PAT asks for highly sophisticated concepts and for electro-mechanic and electro-optic hardware meeting exceptional technological standards. Major parameters entering the link capacity are telescope size, optical transmit power, link distance, and receiver sensitivity. Other aspects are mass, volume, and power consumption of the terminal. Examples for existing space laser communication links include *European Space Agency* (ESA)'s inter-satellite link *Semiconductor Laser Inter-satellite Link Experiment* (SILEX) and a satellite ground link, which was only recently realized between the GEO satellite

 © Eurocontrol, June 2004.

ARTEMIS end ESA's optical ground station *Optical Ground Station* (OGS) at Tenerife.

Although space-to-space links have the attractive advantage of not being influenced by Earth's atmosphere, of the position correlation between satellites in the network, see the figure 4.6 on page 53, it is too much difficult at present due to the expected disproportionate technological and financial effort as compared to alternative schemes with at least one of the communication terminals on ground. Most envisioned quantum experiments require higher flexibility at the receiver due to active polarization control or data analysis, thus it is more reasonable to place the transmitter module in satellite, while the receiver modules stay in easily accessible ground-based laboratories.

Because of their relative stationary, terminals placed on GEO satellites do not require such a highly sophisticated PAT systems as those on a LEO satellite. They would also for long-duration experiments. But on the other hand, the link attenuation and cost are significantly larger for GEO links compared to LEO links. Therefore, when trading GEO-based against LEO-based systems, we would rather accept the more complex PAT system and the limited connection time per orbit and suggest to use a LEO platform for the transmitter terminal for the first experiments.

In the next section, anyways, we will analyze in more details the possible space scenarios, prerequisites and perspectives of satellite-aided QKD.

© Eurocontrol, June 2004.

Section 5

Analysis and Scenarios

5.1 Introduction

According to the analyses of preceding section, one can completely send a single photon in space. Today (June 2004), two groups have succeeded in exchanging keys over free-space ranges greater than 1 km and ongoing experiments show that ranges of 10 and 23 km [**?**] [32] can easily be reached. In all experiments the first step are being taken to reduce the size, mass and power consumption of the equipment primarily to allow portability in the short term and fully automated remote operation in the long term. In the future, one will be able to envisage modern equipment which will allow to exchange photons over 1000 km [39]. One can thus imagine a scenario of distribution of key between the station on the ground and the plane. But how is it done? One can easily know that there are many disadvantages if the station and the plane are communicated directly [35]

- The distance of communication is limited. Therefore, it is necessary to install ground stations of each thousand km to contact the planes. It is not possible because the budget to maintain these stations is too high. Especially, the installation of the ground stations is facing much natural obstacles.
- High attenuation due to atmospheric effects is shown in figure 5.1 on the next page. It is easy to see that the way passed by satellite, BP and AG, is shorter than by the direct communication PG in the zone of atmospheric effects. The light gray zone is full of noise). Thus, the direct communication causes several bad information by lost photons.

To solve these disadvantages, we suggest a scenario of communication using satellite. With this model, there are following advantages [35]

- Easy to cover a space with a network of satellites. Thus one can well solve the problem of distance.
- Ground station may easily be removable or re-installable in short time.
- Point-to-multipoint: a satellite can contact several of ground stations or planes.

© Eurocontrol, June 2004.

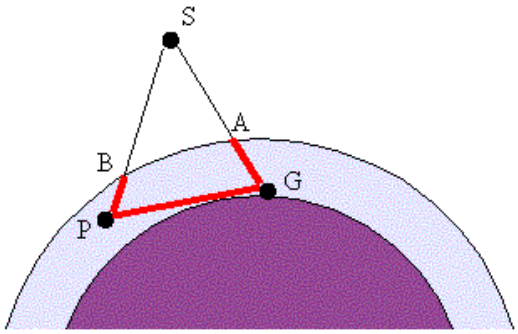


Figure 5.1: Influence of atmosphere on the QKD.

With all these disadvantages and advantages, one can say that the model of satellite communication is ideal. In the following parts, let us propose the key exchange to satellite scenario and also a network of architecture using satellites.

5.2 Key exchange scenario

With first stage, we consider the exchange of key between a ground station and a low earth orbit satellite (800 km). According to [43], there are three options to analyze

- The ground station transmits a key to the satellite
- The satellite transmits a key to the ground station
- The ground station transmits a key to another ground station using the satellite as a mirror

For all the three models, it needs a classical channel which must be able to exchange digital data at high bit rates to allow interactive alignment, time synchronization, key sifting and error correction to be carried out in real time. Ethernet bandwidths (10 MHz) are needed for real-time operation. Lower classical bandwidth would require some time after optical key exchange for the protocol to be completed, thus limiting the number of key bits that could be exchanged on a typical pass. For the optical channel, we suggest telescopes like the following:

- A big telescope on the ground station with a diameter up to 30-100 cm which must be able to track the satellite
- A small telescope on the satellite (10 or 30 cm). With 10cm optics the target of 3 kg may be reached but 30 cm optics will be difficult to build below 5 kg. Thus it is necessary to consider the size of telescope to decrease the cost.

 © Eurocontrol, June 2004.

5.2.1 The ground station transmits a key to the satellite

[43] A typical system is illustrated in figure 5.2.

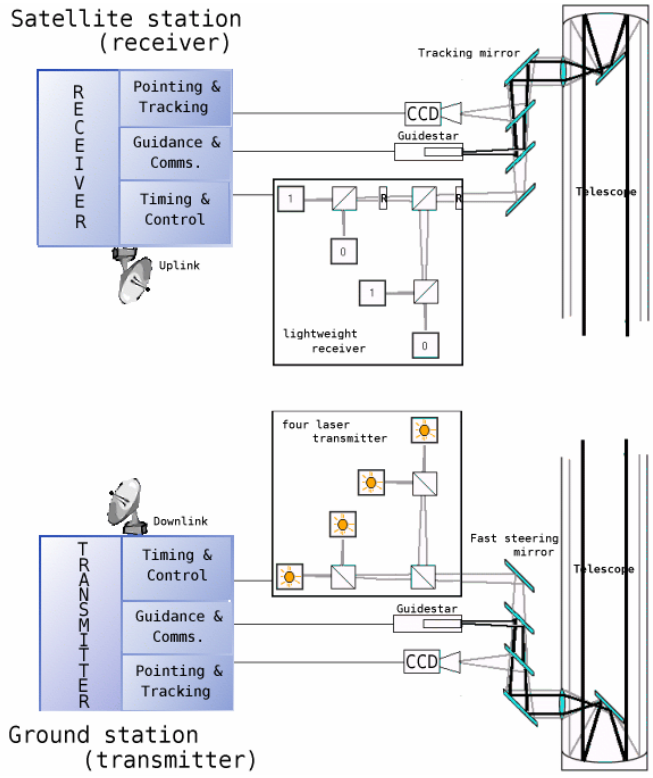


Figure 5.2: (a) Satellite station receiver. This includes a lightweight receiver module, a guidestar laser for ground tracking and a CDD camera to maintain closed loop pointing. An on-board lightweight processor handles the pointing and tracking, time synchronization and key management. (b) The ground station incorporates the compact four-laser transmitter with a high power 'guidestar' laser and pointing tracking CDD.

- *Ground telescope, tracking, pointing and turbulence.* Typically one would use a ground laser expanded to a near-diffraction-limited 30 cm beam. This would imply R ([1]) diffraction spread. To keep such a small spot pointing at the satellite requires a high-speed active pointing scheme correcting for turbulence wander at the ground station. On the satellite the pointing and tracking requirement would be less stringent (100 μR) but both the ground station and the satellite would need to be fitted with laser beacons (guidestars). A suitable point-ahead scheme will be needed as the satellite velocity will take a considerable distance (tens of meters or 20-50 μR) in the time it takes a beacon to reach the ground and a signal to return. This also means that the guidestar beam will not pass through the same column of atmosphere as the up-going signal beam. As most turbulence occurs in the 1 km boundary layer where beam deviation will be at most 50 mm (in a 30 cm wide beam) we expect this will not strongly

[1] R: pulse repetition rate of the system

affect the closed loop pointing. The best space based optical communication experiments are just achieving 2 μR tracking without turbulence and we suspect that from the ground one might achieve 3-5 μR tracking accuracy. This will degrade our effective beam spread to around 6 μR.

- *Satellite optics pointing stability.* We require only that the ground station remains within the field of view of the detectors. The angular field of view θ_o at the output optic is given by

$$\theta_o = \frac{D_d}{f}$$

where D_d is the detector diameter (typically 500 μm) and f is the telescope focal length. For a 10 cm (30 cm) optic $\frac{f}{10}$ telescope the field of view is 0.5 mR (0.17 mR). Tracking accuracy at the satellite is thus not as stringent (>100 μR). With such a wide field of view operation in daylight conditions may be impossible due to excess background light. Reducing the detector field of view and pointing to better than 100 μR may be preferred. When the field of view is less than 100 μR pointing ahead of the image of the ground based guidestar becomes important.

- *Satellite optics rotation stability.* The effective orientation of the satellite would be monitored by measuring guidestar polarization at the ground station and correcting at the ground.

- *Maximum distance.* At 1000 km range loss $TL_g(^2) = 0.00036$ ($\sim$ 34dB) for 10cm satellite optics and $TL_g = 0.00032$ ($\sim$ 25dB) for 30 cm diameter satellite optics, assuming atmospheric transmission $T \sim 0.65$. Setting the maximum loss tolerance at 35dB (for security and error correction reason), the maximum range is just 1100 km with 10cm satellite optics and >3000 km with 30 cm optics.

- *Expected key rates.* According to the formula

$$K = \frac{RMTL_g\eta}{2} \quad (^3)[43]$$

If there are a laser repetition rate of R = 100MHz and M = 0.1 photon per bit, we obtain $K \sim 4500 bits/s$ at 1000 km and $K \sim 1000 bits/s$ at 2000 km for 30 cm satellite optics. As for 10 cm optics this becomes $K \sim 450 bits/s$ at 1000 km.

- *Error rates and loss tolerance.* Background light errors could be a problem when transmitting from populated areas. However, limiting ourselves to 35 dB maximum loss at maximum range implies a maximum background B < 240 counts/s (^{4}) which is easily achieved at night with nanometer bandwidth filters.

In short, with this scenario, there are following significant technical figures:

- Diameter of ground optics: 30 cm

[2] T: atmospheric transmission - L_g: geometric loss

[3] K: expected key exchange rate - M: number of photons per pulse - η: detection system lumped efficiency

[4] B: background count rate per second

 © Eurocontrol, June 2004.

- Technical numbers concerning the satellite

optics diameter	10 cm	30 cm
Ground tracking and pointing	$4\mu R$ diffraction	$4\mu R$ diffraction
Satellite optics pointing ability	$100\mu R$ Locked to ground laser guidestar	$100\mu R$ Locked to ground laser guidestar
weight of telescope	3 kg	5 kg
Satellite optics yaw stability	Corrected from ground	Corrected from ground
Maximum range	1100 km	> 3000 km
Key rate (K)	450 bits/s at 1000 km	4500 bits/s at 1000 km 1000 bits/s at 2000 km
The loss budget (TL_g) at 1000km	< 35 dB	< 35 dB
Error rates	$2-7\%$	$2-7\%$

5.2.2 The satellite transmits a key to the ground station

The satellite optics (transmitter) is shown in figure 5.3 on the next page. The four-laser source can be made extremely compact and lightweight. A beam-splitter picks off a view of the ground for a CCD camera so that closed loop pointing control can be performed. The beam is then expanded to 10 cm to send to the ground. The receiver is in the ground station with a fixed telescope with up to a 100 cm diameter. It too has closed loop tracking but with lower resolution than the transmitter.

- *Ground telescope, tracking and pointing.* To make it easy to track the satellite a field of view $> 100\mu R$ could be engineered. This would require an effective f/5 100 cm telescope with 0.5 mm detectors. Using high numerical aperture relay lenses before the detectors we could reach an effective f/2 telescope (250 μR field of view). In this form daylight background levels will be high and night operation will be preferred. With a large field of view, point-ahead tracking corrections may not be necessary.

- *Satellite optics pointing stability.* With the laser on the satellite we will have to point with an accuracy of 12 μR. This will require the use of an upward pointing beacon laser co-aligned with the ground telescope. The bandwidth of this system should not be high, involving probably drift time-scales of the order of seconds. Thus we could use a slow tip-tilt mirror at an intermediate stage. Placing a tip-tilt mirror at a position where beam diameter is $\sim 25mm$, the $\pm 0.5^o$ stability of the satellite is magnified by a factor of 4. The tip-tilt system thus requires a full-scale tilt of order 34 mR ($\pm 2^o$) and the closed loop needs to operate with an accuracy $< 40\mu R$.

- *Satellite optics rotation stability.* The effective orientation of the satellite would be monitored by measuring polarization at the ground station and

corrected at the ground.

- *Satellite payload and power.* With 10 cm optics the target of 3 kg may be reached.

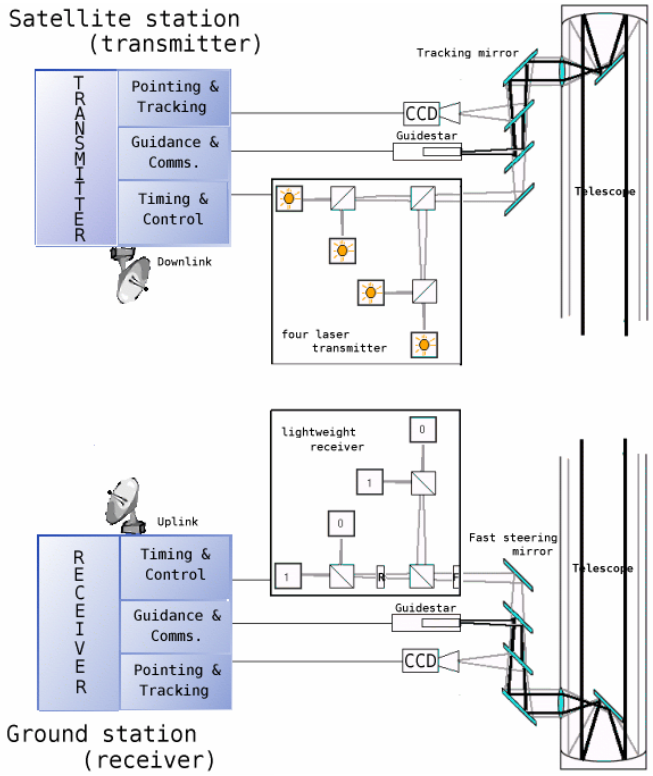


Figure 5.3: (a) Satellite based transmitter. This includes a lightweight laser system using matched lasers and electronic switching between them to select the four polarizations used in the BB84 protocol. Pointing and tracking are controlled to the level by the satellite while a closed loop system incorporating CCD tracking electronics and a tip-tilt mirror controls fine pointing to better than $10\mu R$. (b) Ground station with telescope and boresighted beacon laser. The four-detector receiver design provides a wide field of view ($100\mu R$ at the telescope output).

- *Maximum range.* With 10 cm optics the diffraction spread of a 650 nm beam is of order 12 μR and the ground footprint would be 12 m from 1000 km. This gives a loss in a 100cm diameter telescope at the ground station of $TL_g = 0.0046(\sim 23.5dB)$. With a 50cm diameter telescope $TL_g = 0.0012(\sim 29.3dB)$. With 35 dB maximum tolerable loss the maximum ranges are >4000 km for a 100cm telescope and >2000km for the 50cm telescope. At these higher ranges we have had to take into account the extra loss from atmospheric transmission at low elevation angles in the atmosphere.

- *Expected key rate (at 1000 km range).* The key rate will be limited by the maximum repetition rate of the lasers and the loss. With $R = 100MHz$

 © Eurocontrol, June 2004.

and $TL_g = 0.0045$ we expect a ground key rate at 0.1 photon per bit of $K \sim 6600 bits/s$. For a smaller 50cm ground telescope $K \sim 1600 bits/s$

- *Error rate.* (At a night sky) the error rates due to background light will be low. Again, using a maximum loss of 35 dB implies a maximum background B < 240 counts/s. With suitable filters this may allow operation at night when the satellite is still in sunlight. However, daylight operation is not possible due to the wide viewing angle (100 μR) proposed for ease of tracking in the receiver. Better tracking might allow a smaller field of view and thus limit daylight background.

Summary table performance of the system

- Satellite optics diameter: 10 cm, and weight of telescope: 3 kg.
- Two types of ground telescope

Ground telescope	50 cm	100 cm
Ground tracking and pointing	$> 100\mu R$	$> 100\mu R$
Satellite optics pointing ability	$12\mu R$ Locked to ground laser guidestar	$12\mu R$ Locked to ground laser guidestar
Satellite optics yaw stability	Corrected from ground	Corrected from ground
Maximum range	> 2000 km	> 4000 km
Key rate (K) at 1000km	1500 bits/s	6500 bits/s
The loss budget (TL_g) at 1000km	< 35 dB	< 35 dB
Error rates	$2 - 7\%$	$2 - 7\%$

5.2.3 The ground station transmits a key to another ground station using the satellite as a mirrror

The system includes a pulsed laser system at ground level boresighted with the tracking telescope that acts as a receiver. This laser sends a relatively broad beam up to the satellite. On the satellite there is retro-reflector formed by a simple telescope with a mirror set at its focal point. Before the mirror is a polarization modulator which can encode the required four polarization states onto the retro-reflected beam.

- *Ground telescope, tracking and pointing.* The system can use a relatively high divergence ground based laser beam (100 μR). This only requires that the ground telescope points with 100 μR accuracy at the satellite. The return beam will, however, deviate somewhat from true retro-reflection essentially due to the Doppler effect occurring because of the satellite velocity $V \sim 7km/s$ relative to the velocity of the earth's surface. The deviation angle is of order , corresponding to some $47\mu R$ of deviation

(47 m at the earth's surface for a satellite height of some 1000 km). At first glance, this system is then unworkable as this is much larger than the diffraction spreading ($\sim 12\mu R$) and we would require separate tracking for the laser and telescope separated by varying distances, dependent on range. This can be solved by fitting a biprism element in the satellite optics as shown in figure 5.4 on the facing page. The biprism angle is chosen such that the passage through either side will divert the beam by exactly half the Doppler angle. A light beam entering the retro-reflection system will pass through the opposite side of the biprism on its return, thus suffering a deviation equalling the Doppler angle $\pm\theta$. We will then obtain two return beams, one exactly co-linear with the incoming beam and the other deviated by $+2\theta$. A more detailed analysis shows that, with a typical satellite, this correction scheme will return the light to the ground station within its diffraction spread for most elevations above 50^o. The biprism will effectively halve the returned light.

As the output from the retro-system is $\sim 0.1 photons/bit$ this requires us to have at least $10 photons/pulse$ arriving in the $10cm$ aperture of the satellite optics. The footprint of a $100\mu R$ beam at the satellite is of order $100m$, implying 10^{-6} of the laser power will enter the satellite optics. For a system operating at $100MHz$ repetition this implies $10^{15} photons/s$. This implies a ground laser emitting around $3mW$ of power in $100 - 200 photons/pulse$ at $100MHz$. Power variation with range (and visibility) can be monitored by the satellite based single-photon detector.

- *Satellite optics pointing stability.* In the retro-reflection system we require only that the ground station remains within the field of view of the retro-reflector. This will usually be limited by the polarization switch which will have a limited acceptance angle. Present low voltage $(200V)$ electro-optic switches have a $10mR$ field of view in a $1mm$ beam, translating to $100\mu R$ in an output beam of $10cm$ diameter. However, a larger area liquid crystal device will offer a much wider field of view, up to $20mR$ at the telescope entrance, which may only require pointing of the satellite to an accuracy of a degree. Tracking the ground station is achieved by locking the image of the ground station laser to the centre of a sensitive CCD camera.

- *Satellite optics rotation stability.* The effective orientation of the biprism would have to be maintained normal to the satellite motion. This requires an accuracy of a few degrees. This effect could not be corrected from the ground.

- *Maximun range.* The retro-reflected beam will be diffraction limited when the mirror is at the exact optical focus. For $10cm$ optics this would mean a diffraction spread of $\sim 12\mu R$ and a $12m$ spot on the ground. An extra 50% loss is also inherent in the biprism system. This gives a loss of $0.5TL_g = 0.0023(\sim 26.5dB)$ in a $100cm$ diameter telescope and $0.5TL_g = 0.0006(\sim 32dB)$ with a $50cm$ diameter telescope at the ground station. With $35dB$ maximum loss, the maximum ranges are $> 3000km$ for a $100cm$ telescope and $> 1800km$ for the $50cm$ telescope.

- *Expected key rate (at 1000 km).* The key rate will be limited by the maximum rate of modulation of the retro-reflecting polarization modulator.

 © Eurocontrol, June 2004.

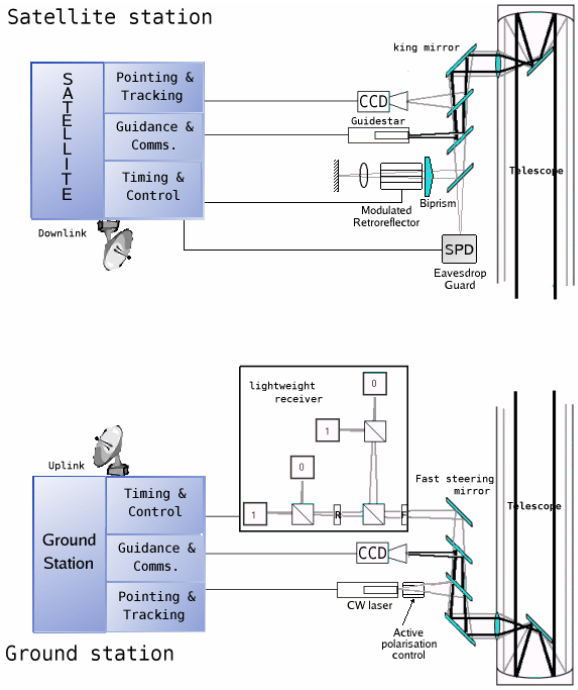


Figure 5.4: (a) Satellite station using a polarization modulating retro-reflector. Doppler shifts due to the relative motion between satellite and ground is compensated by a biprism design. The CCD is used to point the satellite at the ground station with an accuracy set by the field of view of the retro-reflector ($> 100\mu$R). A guidestar laser is used to lock the ground station pointing. (b) Ground station for the retro-reflection system. A bright pulsed laser is roughly collimated to point at the satellite. The guidestar/satellite image in the CCD camera is used for closed loop tracking to within the field of view of the receiver module (100 μR)

Using present technologies this is about $R \sim 10MHz$ in a $10kg$ electro-optic system, $R = 0.5MHz$ in a $0.2kg$ liquid crystal modulator. From the above $0.5TL_g = 0.0023$ and $K \sim 330bits/s$ with $R = 10MHz$ and $K \sim 16bits/s$ with $R = 0.5MHz$. If a future lightweight modulator operating at $100MHz$ is produced, bit rates of $K = 3300bits/s$ can be expected.

- *Error rate.* using a maximum loss of 35 dB implies a maximum background B < 240 counts/s.

Summary table performance of the system ground station transmits a key to another ground station using the satellite as a mirror

- Satellite optics diameter: 10 cm. Satellite payload:
  - (a) Modulator < 5 kg, R = 0.5 MHz
  - (b) Modulator 11 kg, R = 10 MHz
  - (c) Future mod < 5 kg, R = 100 MHz

- Two types of ground telescope

Ground telescope	50 cm	100 cm
Ground tracking and pointing	$> 100\mu R$ detector limited	$> 100\mu R$ detector limited
Satellite optics pointing ability	$100\mu R$ Locked to ground laser guidestar	$100\mu R$ Locked to ground laser guidestar
Satellite optics yaw stability	Corrected from ground	Corrected from ground
Maximum range	1800 km	3300 km
Key rate (K) at 1000km	(a) 16 bits/s (b) 330 bits/s (c) 3300 bits/s	(a) 16 bits/s (b) 330 bits/s (c) 3300 bits/s
The loss budget (TL_g) at 1000km	< 35 dB	< 35 dB
Error rates	$2 - 7\%$	$2 - 7\%$

In conclusion, with these three scenarios we can completely send a sequence of single photons between the ground station and the satellite. Therefore, we can imagine entirely a system for secure key exchange from the ground to satellite using quantum crytography. Moreover, nowadays, using position systems: GPS of United States of America, Galelio of Europe in the future... we can easily locate an object in space with errors of a few centimetres [2]. So it does not need the guidestar laser for tracking and CCD camera to maintain closed loop pointing. That's why the weight of satellite is lighter. Thus the satellite network project for secure key exchange in space is more feasible. Afterwards, we will consider some suggested architectures to create a satellite network in the following section.

5.3 Satellite network

According to three scenarios for secure key exchange in free-space, it is not difficult to exchange the key between two points in free-space. The problem suggested here is the cover of an enormous space (European space). Thus we have need a satellite network to cover it, shown in figure 5.5 on the next page and in figure 5.6 on the facing page. To install this network, there are several questions to answer:

- It needs how much satellite to form this network?
- How the satellites and the station are communicated?

In this part, we propose some models to create a satellite network. There are two choices [35]:

- Ground-Based transmitter terminal: key is transmitted from the ground to the satellite

 © Eurocontrol, June 2004.

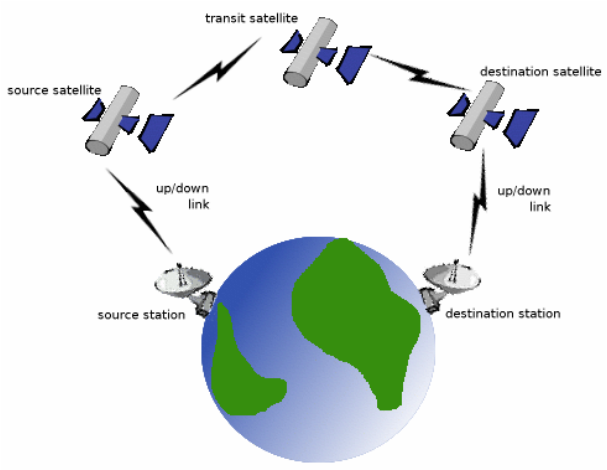


Figure 5.5: Satellite network

- Space-Based transmitter terminal: key is transmitted from the nal optique satellite to the ground or to another satellite

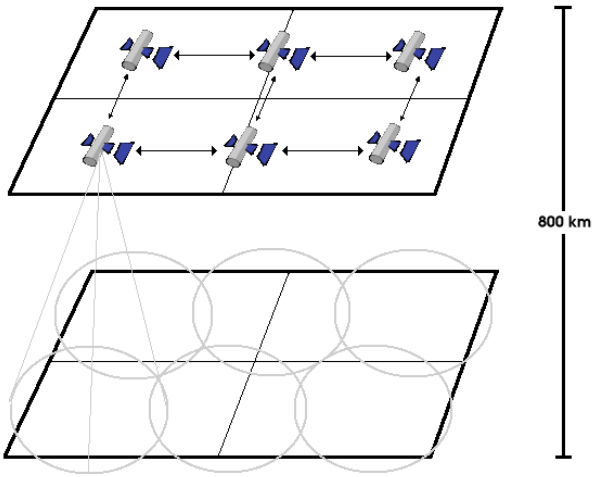


Figure 5.6: Space covered by satellite network

Normally, with a satellite of the altitude (a = 800 km) and its maximum range (d) one can calculate the surface covered on the ground with a diameter (2r), shown in figure 5.7 on the next page [28]

$$r = \sqrt{d^2 - a^2} \tag{5.1}$$

Really, when one forms a satellite network to cover an enormous surface, one cannot install the satellites with the distance 2r because there is a small unknown area (space black), shown in figure (a) 5.8 on the following page.Each satellite covers only one surface of a hexagon registers in the circle, shown in figure (b) 5.8 on the next page.

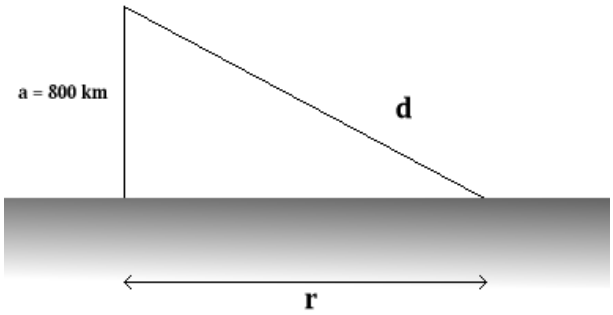


Figure 5.7: Space covered by a satellite

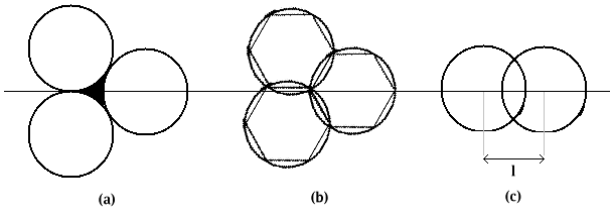


Figure 5.8: Distance between two satellites of network

Therefore, the distance between two satellites is l, shown in figure (c) 5.8

$$l = r\sqrt{3} \tag{5.2}$$

Theoretically, the radius of the Earth is of 6378km and the altitude of satellite is of 800 km. Therefore, the radius of satellite orbit is of 7178km and it needs n satellites to cover a surface of width l km, shown in figure 5.9 on the next page

$$n = \frac{2\pi 7178}{l} \simeq \frac{45100}{l} \tag{5.3}$$

In two following parts, it is the same calculation for each scenario

5.3.1 Ground-Based Transmitter Terminal

Distribution key from ground station. There are remarks following [35]

- Advantages
  - easily accessible source
- Disadvantages
  - high attenuation due to atmospheric effects
  - distance limited

 © Eurocontrol, June 2004.

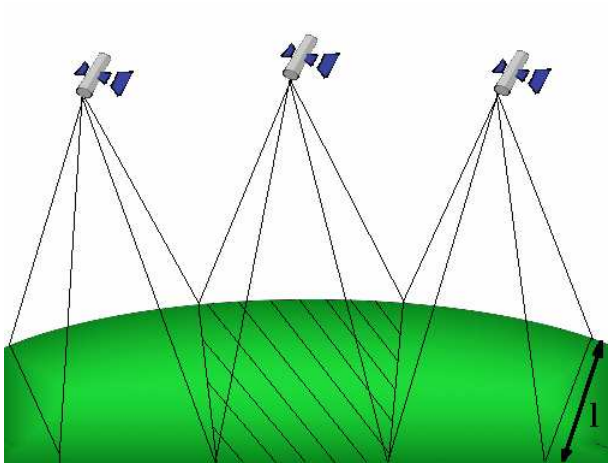


Figure 5.9: Satellites network

According to the part (5.2), there is some parameters technical, shown in table 5.1

Table 5.1: Maximun range (d) of two types of satellite's optics diametter

Optics diametter	10 cm	30 cm
Maximum range	$\sim 1000km$	$\sim 3000km$

Analysis 5.3.1. *The photon is sent from the ground station to the 10 cm of satellite's optics diametter*

Follows table 5.1 and equation 5.1 on page 67, the maximum distance d = 1000 km, the radius couvered r = 600 km. Thus, the distance between two satellites l $\simeq$ 1040 km (equation 5.2 on the preceding page) and it needs $\sim$43 satellites (equation 5.3 on the facing page) to cover a surface of width 1040 km.

Analysis 5.3.2. *The photon is sent from the ground station to the 30 cm of satellite's optics diametter*

Follows table 5.1 and equation 5.1 on page 67, the maximum distance d = 3000 km, the radius couvered r = 2890 km. Therefore, the distance between tow satellites l $\simeq$ 5010 km (equation 5.2 on the preceding page) and it needs $\sim$9 satellites (equation 5.3 on the facing page) to cover a surface of width 5010 km.

5.3.2 Space-Based Transmitter Terminal

Distributing key from satellite. Because the optics of ground station is larger than the optics of satellites, the distance is further and spaces covered by satellite is also broader. There are remarks following [35]

- Advantages
  @

  - more flexible
  - golbal distribution of key
  - proof-of-concept (space qualification)
- Disadvantages
  - More complicated

According to the preceding part, there is some parameters technical, shown in table 5.2

Table 5.2: Maximun range (d) of two types of ground station's optics diameter

Optics diameter	50 cm	100 cm
Maximum range	$\sim 2000km$	$\sim 4000km$

Analysis 5.3.3. *The photon is sent from the satellite to the 50 cm of ground station's optics diametter*

One has the maximum distance d = 2000 km (table 5.2) and the radius couvered r = 1930 km (equation 5.2 on page 68). Thus, the distance between tow satellites l $\simeq$ 3174 km (equation 5.2 on page 68) and it needs $\sim$14 satellites (equation 5.3 on page 68) to cover a surface of width 3174 km.

Analysis 5.3.4. *The photon is sent from the satellite to the 100 cm of ground station's optics diameter*

Follows table 5.1 on the preceding page and equation 5.1 on page 67, the maximum distance d = 4000 km, the radius covered r = 3920 km. Therefore, the distance between tow satellites l $\simeq$ 6790 km (equation 5.2 on page 68) and it needs $\sim$7 satellites (equation 5.3 on page 68) to cover a surface of width 6790 km.

In brief, the distance of optical channel is really limited. There is always a big problem to send photons for a long distance free space. Thus, the scenario of distribution key from the satellite to the ground station is the best choice because it is easy to install a large telescope at the ground station with less low budget.

 © Eurocontrol, June 2004.

WP II

ATN and QKD Scenarios

© Eurocontrol, June 2004.

Summary and Conclusions

This part summarizes the conclusions of the second step of this study. These conclusions are made explicit in the following sections.

Summary

- Chapter 6 on page 75, *"ATN Communications secured with PKI"*, describes several scenarii for the integration of Quantum Key Distribution (QKD) in the Aeronautical Telecommunication Network (ATN):
  - for Air/Ground (A/G) telecommunications;
  - for Ground/Ground (G/G) telecommunications.

  This chapter emphasizes on the requirement of incrementality of the proposed solutions and, of course, on the minimization of the costs.
- Chapter 7 on page 93, *"QC Communication Protocols"*, describes methods for resolving one of the main problems of telecommunications, that is the authentication of the other party.

Partial Conclusions

- One must be aware that WP2 has been conducted with the assumption that all QKD equipments were already available. Even if quantum technology is fastly evolving, the current available QKD equipments do not allow all the scenarii to be implemented.
- If all the QKD equipments were available, then numerous scenarii are available to secure the ATN. QKD optic fiber technology can be used to secure G/G communications. Otherwise, QKD freespace technology may be used for A/G communications. The most interesting way of truly securing the ATN would require a satellite network.
- If ATN has to be secured, and it will be secured, all communications endpoints have to receive encryption keys. Distributing a key to an aircraft coming from outside Europe or from an untrustable country would require radio communications that could be eavesdropped. The same occurs for aircraft standing on the tarmac at airports and which are not wired to the terminal. In these case, Freespace QKD could provide a solution that could not be eavesdropped.

© Eurocontrol, June 2004.

- We can consider a QKD system for ATN Network as the *Quantum Confidentiality Key Infrastructure* (QCKI) which provides confidential sharing of encryption keys between two endpoints replacing PKI in a progressive manner.
  - For instance, a subnetwork such as an airport could be QCKI-equipped meanwhile the other parts of the ATN may continue to use classical PKI.
  - For instance, airport control tower may be equipped to distribute keys to all airplanes standing at the airport for signature of A/G communications or Air Identification Tag (AIT).
  - For instance, QCKI could be used tu unconditionnaly secure links between some ATN subnetworks and this may be incrementally applied to all links.

  There are many ways to *locally insert* QCKI inside the ATN. The last, but very expensive step, would be to use satellites.
- We mention several possibilities of key distribution:
  - Single-photon source Ground-based QCKI, see page 82.
  - Single-photon source Aircraft-based QCKI, see page 83.
  - Single-photon source Satellite-based QCKI, see page 84.
  - Entangled-photon source Ground-based QCKI, see page 85.
  - Entangled-photon source Aircraft-based QCKI, see page 86.
  - Entangled-photon source Satellite-based QCKI, see page 87.
- *Environmental impact.* We did not see any environmental impact since the QKD quantum equipments do not produce anything.
- *Health concerns.* QKD technology uses lasers. However, it is faint pulse lasers which are not supposed to hurt people.

WP3 Future Works

- To provide visual animations to illustrate one or two scenarii that we have explored.
- To provide a animated implementation of BB84.
- To build a follow-up proposition to be submitted to the CARE manager. Its main characteristics are:
  - It must provide an effective realization within two years.
  - We will have a Quantum Physics laboratory specialized in lasers as a partner for the equipment items of the project.
  - It must be a step towards the integration of QKD inside the ATN.
  - It could be a way for the authentication of Air identification Tag (AIT) which has been developed at Eurocontrol with the cooperation of the Graz University of Technology in Austria.

© Eurocontrol, June 2004.

Section 6

Introducing QC in ATN

6.1 ATN Communications secured with PKI

The figure 6.1 summarizes communications between the *Aeronautical Telecommunication Network* (ATN) entities.

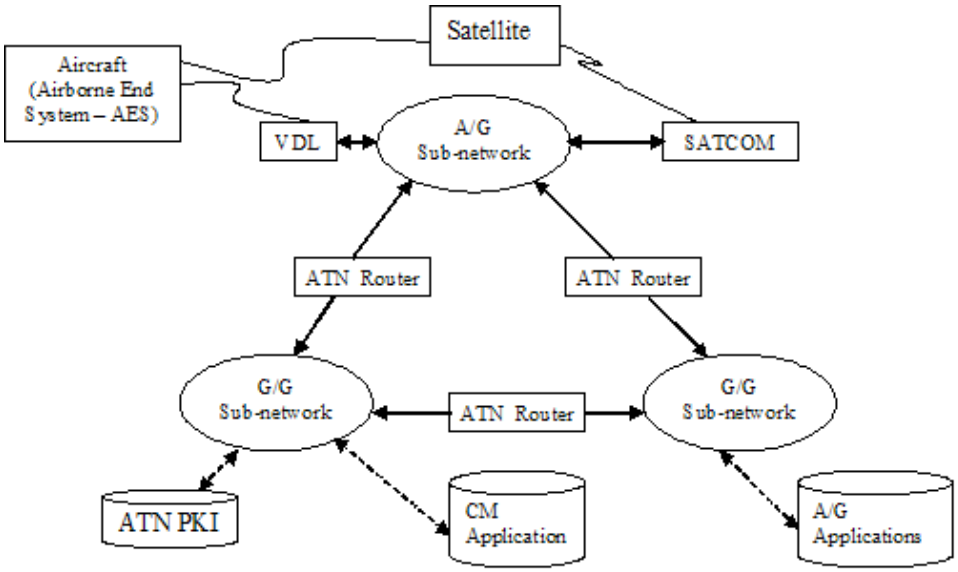


Figure 6.1: ATN communications network.

ATN Applications can be categorized into two main categories [27]:

- *Air/Ground* (A/G) Applications corresponding to Sub-Volume 2 of SARPs.
- *Ground/Ground* (G/G) Applications corresponding to Sub-Volume 3 of SARPs.

© Eurocontrol, June 2004.

The *Context Management Application* (CMA) is one of the A/G Applications. CMA provides the mechanism for an *Airborne End System* (AES) to log on the ATN Network in order to communicate and use the A/G Applications and Services required and supported by the AES.

In general, the ATN Security for G/G Application employs solutions similar to those used to protect the "wired-world" Internet. As for A/G Applications, the use of wireless data link in A/G Applications introduces a new set of threats on the operational safety of an aircraft.

ICAO has determined that denial of service, masquerade, and modification of information are the primary threats for A/G Applications. We can summarize the Security Requirements for ATN, cf. section 2.3 on page 20:

- Authentication of Message Source.
- Message Integrity Check.
- Authentication of the source of routing informations.

Analysis 6.1.1. *As such, the security requirements developed by ICAO only address data integrity and peer entity authentication. However, the basic ICAO security framework can be used to protect user information. The ATN security architecture based on Public Key Infrastructure (PKI) is described in Sub-Volume 8 (Security Services) of SARPs.*

In the secure ATN framework, when an AES wants to communicate with a A/G Application at *Ground Station* (GS), for instance the CPDLC Application[1], normally, the AES and GS will cooperate to execute a basic scenario like the following:

- *Step 0:* Initialization of ATN's PKI services for ATN entities who want to take part in secure communications such as Airborne End System (AES), Context Management Application (CMA), CPDLC Application.
- *Step 1:* AES creates a CM Logon CPDLC Request and sends it to CMA.
- *Step 2:* CMA sends a CM Logon CPDLC Response back to AES.
- *Step 3:* AES and CPDLC Application compute a common secret Session Key.
- *Step 4:* AES and CPDLC Application protect their exchanged messages by using this secret Session Key

The table 6.2 on the facing page shows this scenario in more detail.

[1] CPLDC: Controller-Pilot Data Link Communications

 © Eurocontrol, June 2004.

	Airborne End System (AES)	**Context Management Application (CMA)**	**CPDLC Application (CPDLCA)**
Step 0 Initialization of	- AES Identity - AES Private Digital Signature (DS) Key - AES Private Key Agreement (KA) Key	- CMA Identity - CMA Private KA Key	- CPDLC Identity - CPDLC Private KA Key
Step 1 CM Logon Request	- creates CM CPDLC Logon Request using AES ID, CPDLCA ID, time.. - signs on CM Logon Request using AES DS Pri. Key - sends CM Logon Request to CMA	- invokes PKI services for retrieve AES certificates, CPDLCA certificates - authenticates AES's CM Logon Request using AES's DS - generates the CMA Session key using AES Pub. KA Key, CMA Pri. KA Key..	
Step 2 CM Logon Response	- computes CMA Session Key using CMA Pub. KA Key, AES Pri. KA Key.. - authenticates CM Logon Response by CMA's MAC	- generates CM Logon Response using CMA's Pub. KA Key, CPDLC's Pub. KA Key, CMA Session Key, CMA's MAC - sends CM Logon Response back to AES	
Step 3 Create CPDLC Session Key	- computes CPDLC Session Key using AES Pri. KA Key, CPDLC Pub. KA Key..		- computes CPDLC Session Key using AES Pub. KA Key, CPDLC Pri. KA Key..
Step 4 Exchange protected messages	- protects exchanged messages using CPDLC Session Key	- protects exchanged messages using CPDLC Session Key	

Figure 6.2: Based-PKI secured A/G communications.

© Eurocontrol, June 2004.

77

In the above scenario, AES holds two secret Session Keys: CMA Session Key and CPDLC Session Key. The first one is used for the protected communication with CM Application and the other is used for the protected communication with a CPDLC Application.

In the current situation of ATN, this scenario above is executed by the supporting of ATN's PKI, which have to provide the following Cryptographic Schemes:

- Encryption Scheme: Asymmetric or Symmetric Encryption.
- Digital Signature Scheme: Asymmetric Encryption and Hash Function.
- Key Agreement Scheme: Asymmetric Encryption.
- Message Authentication Code Scheme: Hash Function.

Analysis 6.1.2. *The introduction of PKI in A/G exchanged messages will significantly increase the overhead on the band-limited communication channels, for example, a classical X.509 certificate is about 20Kb*[2]*. We must have some solutions, such as compression, in order to minimize the size of secured messages.*

Analysis 6.1.3. *Typically, the Certificates Revocation Lists (CRL) are very large, therefore, CRLs should not be transmitted to the AES over band-limited A/G links. In order to overcome this problem of CRLs, the Private Keys for AES and GS Applications should be short-lived and the lifetime of these keys should be for the duration of a flight. Hence, as the AES will normally be located within physically secure boundaries controlled by ATN, one option can be to manually upload the keys in the AES before flight.*

6.2 Scenario of QKD in ATN

It is very important that any solution, any improvement of the security must be done in the framework of the ATN construction. It must be fully compatible with ATN and it must be incremental.

We can consider a QKD system for ATN Network as the *Quantum Confidentiality Key Infrastructure* (QCKI) which provides confidential sharing of encryption keys between two endpoints.

As we have seen, the main drawbacks of QKD technology are constraints of distance in the case of optic fiber (130km) or freespace (23km) and constraints of sight-of-line communication in case of freespace QKD technology .

Therefore, if we want to construct an effective QCKI, we must consider two important concepts: *quantum relay* and *QKD data relay*. We need to distinguish QKD data relay from quantum relay.

A quantum relay would redirect and/or manipulate qubit states without actually measuring (reading) them. By contrast, a QKD data relay system is a network apparatus able to establish a secure communication using QKD technology with the previous element of the chain and another secure communication with the following element of the chain. It is a QKD data relay system with the following characteristics:

[2]Kb : K bytes = 1024 bytes

 © Eurocontrol, June 2004.

- Relay k establishes an encrypted radio communication link with relay k-1 based on a shared QKD key.
- Relay k receives encrypted data from relay k-1.
- Data are decrypted and stored in the memory of relay k.
- Relay k establishes an encrypted radio communication link with relay k+1 based on a shared QKD key.
- Data in memory are encoded and sent to relay k+1.

As we have already mentioned, the ATN Network have two main categories of applications: Air/Ground (A/G) Applications and Ground/Ground (G/G) Applications. Now, we will suppose that all current necessary physical equipments of QKD technology are perfect. And let us see the scenarii for the integration of QCKI in each type of ATN applications.

6.2.1 QCKI for A/G Applications

As we know, one of main drawbacks of the ATN's PKI is the band-limitation of A/G links. In the case of AES located in European airports, we can use PKI to distribute keys to AES on the ground before takeoff. But with PKI, it seems to have no solution in the case of AES entering the European sky. QCKI may be a better candidate for this case because his flexibility.

The *Quantum Confidentiality Key Infrastructure* (QCKI) is responsible of providing confidential sharing of encryption keys between two endpoints. In ATN A/G Applications, one endpoint is always an aircraft (AES) and the other can be any Ground Station (GS) which is connected with the ATN Network.

Normally, the selected quantum channel must be a free-space quantum channel because aircrafts can be in the sky. In the case of aircraft on the ground, one can use fiber-based channels instead of free-space channels if the aircraft is wired to the airport infrastructure. Otherwise, if the aircraft is on the tarmac with no physical link to the airport infrastructure, freespace QKD technology can be used.

With the support of QCKI, an aircraft will be able to easily establish a protected communication with A/G Applications supported by the ATN Network as the following basic scenario, see figure 6.3 on the next page.

© Eurocontrol, June 2004.

	QCKI	**Airborne End System (AES)**	**CM Application (CMA)**	**CPDLC Application (CPDLCA)**
Step 0 Initialization	- distributes a quantum secret key for AES and CMA	- receives the Quantum CM Key Session Key from QCKI	- receives the Quantum CM Session Key from QCKI	
Step 1 CM Logon Request		- encrypts CM Logon Request using QCM Session Key - sends to CMA	- checks CM Logon Request using QCM Session Key	
Step 2 CM Logon Response		- checks CM Logon Response using QCM Session Key	- encrypts CM Logon Response using QCM Session Key - sends to EAS	
Step 3 Distribute CPDLC Session Key	- distributes a quantum secret key for AES and CPDLCA	- receives the QCPDLC Session Key from QCKI		- receives the QCPDLC Session Key from QCKI
Step 4 Exchange protected messages		- uses QCPDLC Session Key in order to protect exchanged messages		- uses QCPDLC Session Key in order to protect exchanged messages

Figure 6.3: Secured A/G communications using QCKI

© Eurocontrol, June 2004.

QKD technology have specific characteristics. Hence, if we want to construct an effective QCKI, we must know scenarii in which the QCKI can cooperate with A/G Applications. According to the architecture of the QCKI, i.e the ways of arrangement of the transmitter and the receiver, also the type of photon sources, i.e single-photon source or entangled-photon source, we can imagine the following possible scenarii of using the QCKI in the ATN Network:

- Single-photon source Ground-based QCKI, see page 82.
- Single-photon source Aircraft-based QCKI, see page 83.
- Single-photon source Satellite-based QCKI, see page 84.
- Entangled-photon source Ground-based QCKI, see page 85.
- Entangled-photon source Aircraft-based QCKI, see page 86.
- Entangled-photon source Satellite-based QCKI, see page 87.

- **Single-photon source Ground-based QCKI.**
  The single-photon transmitter is placed at the GS. A straight laser uplink using BB84 protocol to one receiver on the AES can be used to perform the negotiation of the sharing secret key, see figure 6.4.

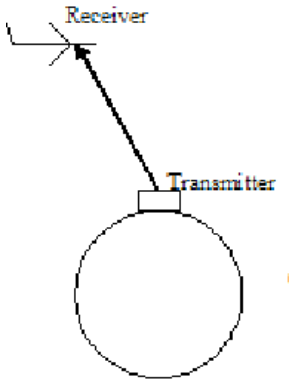


Figure 6.4: Ground-based QCKI with single-photon source

We can also use a satellite which acts as a quantum relay space station, see figure 6.5.

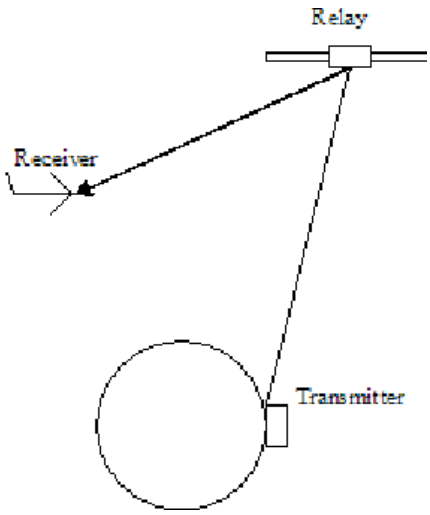


Figure 6.5: Ground-based QCKI with single-photon source

Moreover, it is also possible to use fiber-based technology if aircraft are on the ground in European airports. In this case, the key is distributed before the takeoff of the aircraft.

 © Eurocontrol, June 2004.

- **Single-photon source Aircraft-based QCKI.**
  Each aircraft is equipped by a single-photon transmitter. A straight down-link using BB84 protocol to a receiver on the GS can be used to perform the negotiation of the sharing secret key, see figure 6.6.

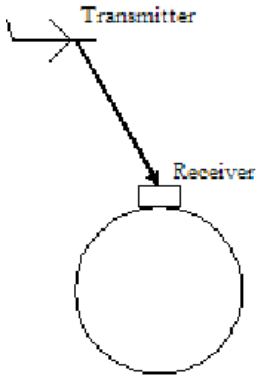


Figure 6.6: Aircraft-based QCKI with single-photon source.

We can also use a satellite as quantum relay space station, see figure 6.7.

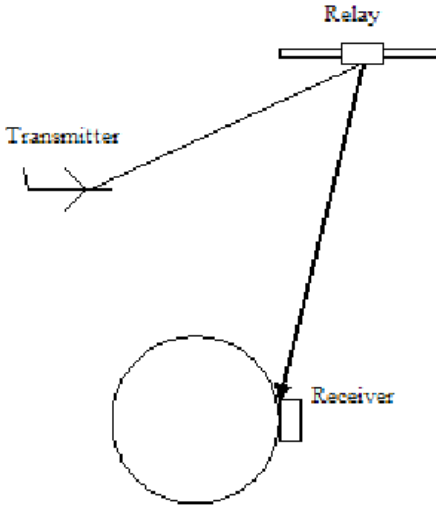


Figure 6.7: Aircraft-based QCKI with single-photon source.

Here too, it is possible to use fiber-based technology if aircraft are on the ground in European airports to distribute keys before the takeoff of the aircraft.

- **Single-photon source Satellite-based QCKI.**

  The single-photon transmitter is placed on the satellite. This case seems more complex because it is impossible to directly negotiate a shared key between AES and GS using QKD technology. It must do the following, see figure 6.8.

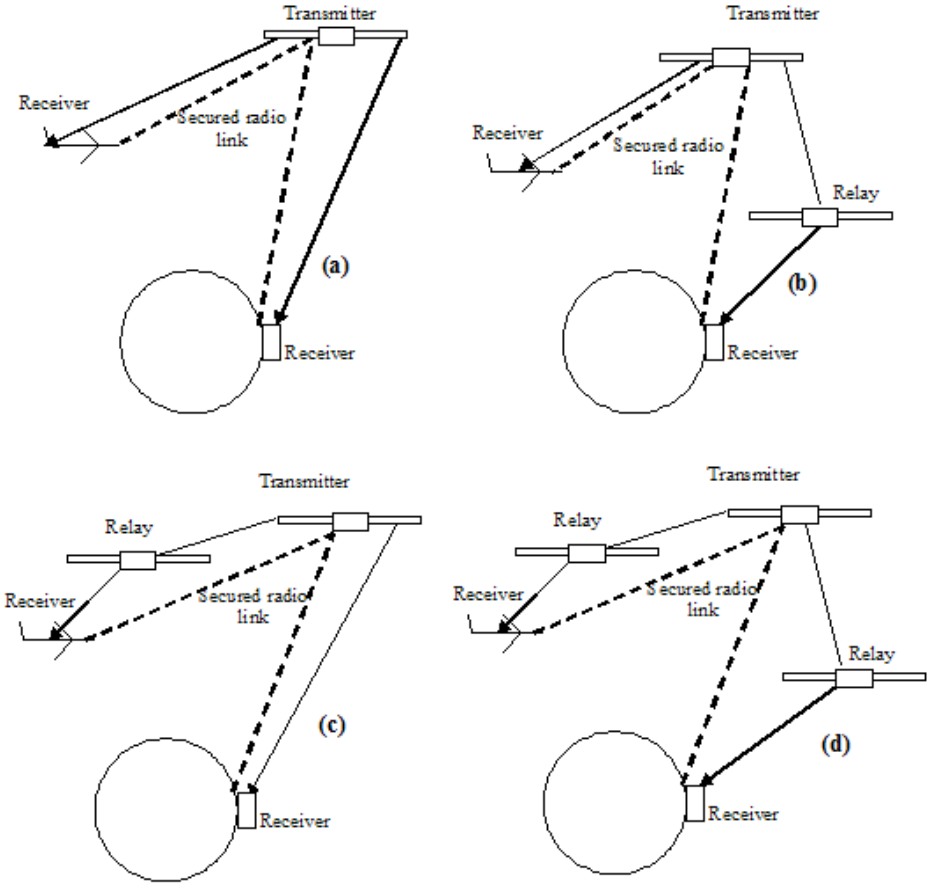


Figure 6.8: Satellite-based QCKI with single-photon source.

The scenario is:

- A satellite distributes a quantum secret key K1 for GS. Using this key K1 as the session key, this satellite and the ATN Network establish a secure radio communication link COM1.
- This satellite distributes an other quantum secret key K2 for AES. Using the key K2 as the session key, this satellite and AES establish a secure radio communication link COM2.
- The ATN Network and the AES negotiate a sharing secret session key by using secure communication links COM1 and COM2.

As such, in fact, the single-photon source satellite-based QCKI can be considered as a satellite-based QKD data relay system.

 © Eurocontrol, June 2004.

- **Entangled-photon source Ground-based QCKI.**

  The transmitter of entangled photon pair is placed on GS. Here, one of the photons of the entangled pair is detected right at GS and thus the entangled photon source is used as a triggered source for single photons toward the AES, see figure 6.9.

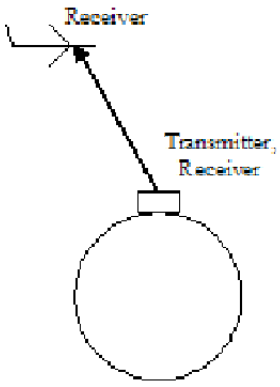


Figure 6.9: Ground-based QCKI with entangled-photon source.

The satellite which acts as a quantum relay station can take part in this scenario, see figure 6.10.

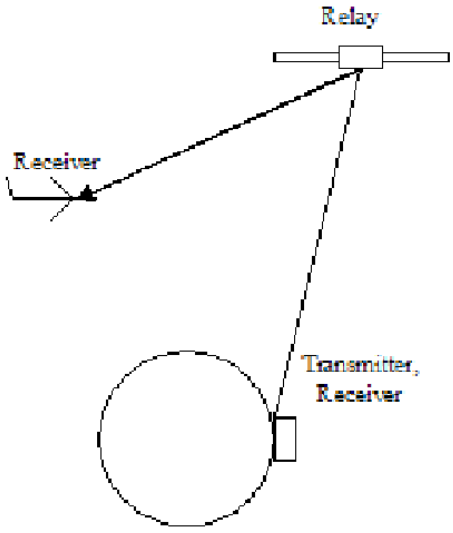


Figure 6.10: Ground-based QCKI with entangled-photon source.

This solution is not very different from the *Single-photon source Ground-based QCKI*, page 82. Only the QKD technology is different.

- **Entangled-photon source Aircraft-based QCKI.**
  The transmitter of entangled photon is placed on aircrafts. Here, one of the photons of the entangled pair is detected right at this aircraft and thus the entangled photon source is used as a triggered source for single photons toward GS, see figure 6.11.

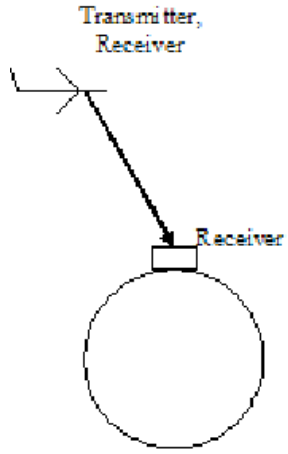


Figure 6.11: Aircraft-based QCKI with entangled-photon source.

The satellite which acts as a relay station can take part in this scenario, see figure 6.12.

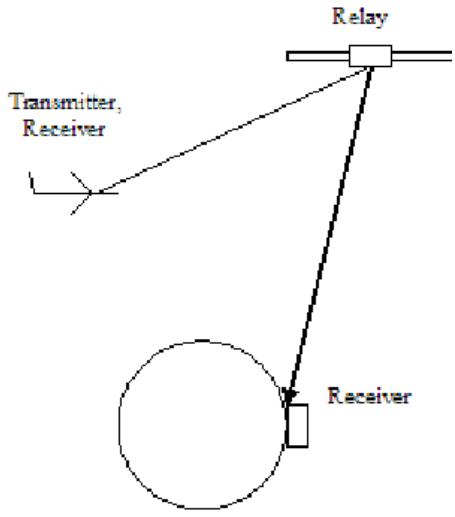


Figure 6.12: Aircraft-based QCKI with entangled-photon source.

This solution is not very different from the *Single-photon source Aircraft-based QCKI*, page 83. Only the QKD technology is different.

 © Eurocontrol, June 2004.

- **Entangled-photon source Satellite-based QCKI.**

  The transmitter of entangled photon pairs is placed on satellites. This is the most interesting use of entangled-photon technology. In the most simplest scenario, the sharing secret key between a AES and a GS can be established by pointing each of the photons of an entangled pair either toward the AES and the GS, see figure 6.13, item (a). Another set of satellite-based relays can be used to further distribute the entangled photons to AES and GS, see figure 6.13, item (b), (c) and (d). In these scenarii, AESs can be on the ground or in the sky.

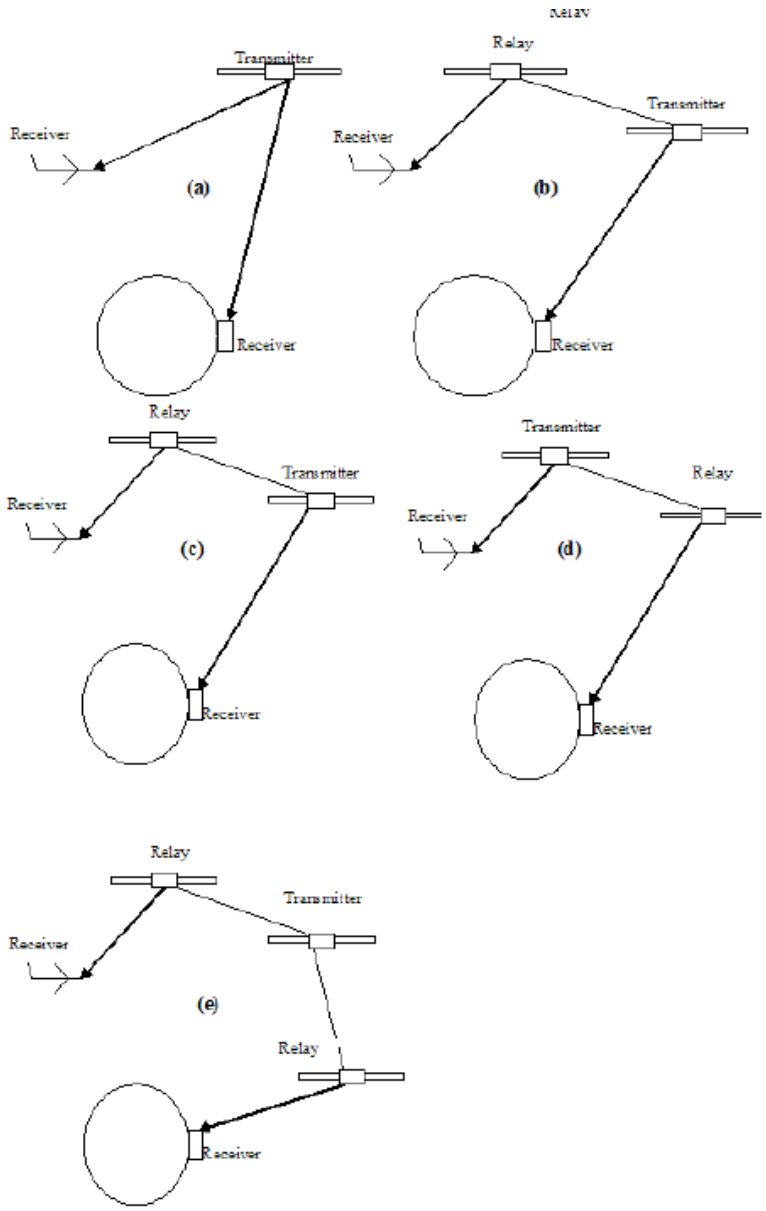


Figure 6.13: Satellite-based QCKI with entangled-photon source.

Analysis 6.2.1. *In all the scenarii above, if we use QKD data relays instead of quantum relays (which do not exist), the model of these scenarii does not seem to require strong modifications. But there would be many changes in the technical equipment and and in the protocols.*

Analysis 6.2.2. *With our current knowledge of the ATN network, we can recognize that the use of QKD technology do not imply any significant changes in the framework of ATN A/G Applications. It is just the another way to securely distribute encryption keys without the using of a (heavy) PKI system.*

6.2.2 QCKI for G/G Applications

Here we describe a basic scenario for protected communications enhanced by QKD technology between two ATN Sub-networks. The scenario can be described as follows:

- *Step 1.* QCKI distributes a Quantum Session Key for two gateways (endpoints) of two ATN Sub-networks.
- *Step 2.* These two ATN Sub-networks use this Quantum Session Key for protecting messages traffic that will transit through the Internet within IPSec tunnels.

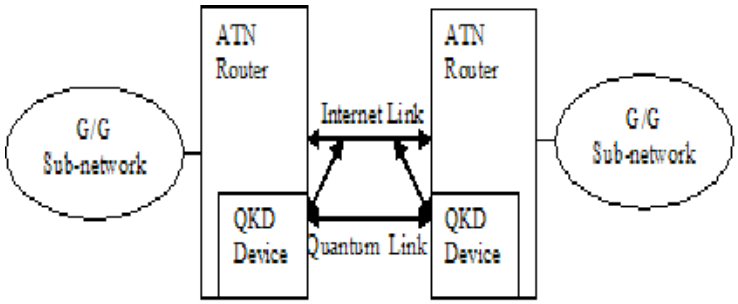


Figure 6.14: Fiber-based QKD between two G/G Subnetworks.

In ATN G/G Applications, the QCKI will provide confidential sharing of encryption keys between two gateways of ATN Sub-networks on the GS. These gateways are in charge of establishing a secure communication using this quantum secret key. As such, we will take advantages of QKD technology into G/G communications by employing solutions similar to those used to protect the "wired-world" Internet, but in which the secret key distribution will be done using QCKI instead of classical technologies such as trusted courier, Diffie-Hellman key exchange, or every Public Key Cryptography algorithm.

There are two main approaches: Ground-based QCKI or Satellite-based QCKI. An aircraft on the ground can also be considered as a gateway of one ATN Sub-network, therefore, the scenarii of Satellite-based QCKI can be completely like those described in A/G Applications, see figure 6.8 on page 84 and figure 6.13 on the preceding page.

 © Eurocontrol, June 2004.

As for a Ground-based QCKI, beside of the same scenarii described in A/G Applications (review figures 6.4 and 6.5 on page 82 and figures 6.9 and 6.10 on page 85), we have one more choice because in this case, we can easily use fiber-based channels instead of free-space channels.

A possible requirement of fiber-based QCKI scenarii is the re-use of existing optic fiber infrastructures and classic-repeater stations with their characteristic distance. Figure 6.14 on the preceding page shows the simplest QCKI-based secure communication between two ATN Sub-networks. In general, there are 2 distinct communications: one is a fiber-based QKD direct link with the BB84 protocol and the other is classical TCP/IP connection using the IPSec protocol which is one of the most current proven and trusted protocols for securing communications. Based on this idea, the DARPA in USA is trying to build a such quantum network, the BBN network. Basically, the BBN network is a classical *Virtual Private Network* (VPN) in which the key distribution and key renewing is done using QKD devices instead of classical technologies such as Diffie-Hellman key exchange. The main benefit of an IPSec VPN is that the corporation has complete control over the robust security policy such that someone attaching to a LAN has all the privileges of a local LAN user and all applications work transparently. Therefore, by using QKD technology for the problem of key distribution and key renewing, the BBN network becomes a totally secured network.

The simplest QKD-based secured communications as above are limited by constraints of distance and sight-of-line communication in the case of Free-Space QKD technology. In order to overcome these drawbacks, one may use quantum relay or QKD data relay stations. There are some solutions [11, 17] such as the using of ground-based QKD data relays, see figure 6.15, or space-based QKD data relays, see figure 6.16 on the next page.

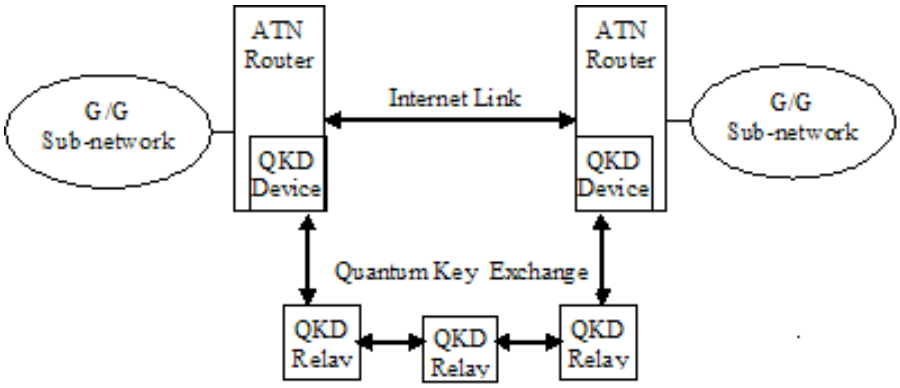


Figure 6.15: QKD relays between two G/G Subnetworks.

As useful as a QKD-relays link may be, it still suffers from another striking drawback because an isolated point-to-point link is subject to simple denial-of-service attacks such as active eavesdropping or cutting the QKD link. This drawback can be mitigated by organizing a number of QKD links into QCKI. The figure 6.17 on page 91 shows a QCKI in highly schematic form.

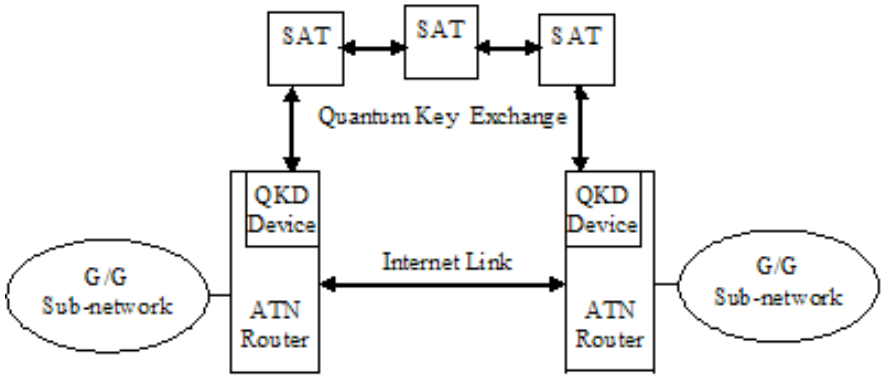


Figure 6.16: Satellite-based QKD between two G/G Subnetworks.

6.2.3 A proposal QKCI for ATN Network

As we know, the use of satellites is the most significant, but also expensive investment. Although costly to deploy and to maintain, it still seems a unique solution for a stable long-distance QCKI. A satellite-based QCKI can overcome the principle limitation of Earth-bound technology, i.e., the range of the order of 150km afforded by both optical fiber and by terrestrial free-space links because of reduced influence of atmospheric turbulence. Therefore, the satellite-based QCKI allows us thinking about the preferred configuration for global QCKI.

Currently, QKD equipments are not standardized. But if the quantum equipments are perfect and standardized, the use of QKD technology will become easy. In fact, we can imagine a ATN's QKCI as following, see figure **??** on page ??:

- Each European airport must support a *Quantum Access Point* (QAP) which is securely attached to the ATN Network and acts as the QKD gateway in order to access into the ATN Network.
- There are no needs to have QKD fixed links between QAPs. Each QAP is independent from each other but is strictly bounded with ATN Network.
- ATN's QKCI is the integration of ground-based QKCI, aircraft-based QCKI and satellite-based QCKI, i.e., QAPs can be placed on the ground, on the satellite or event on the aircraft. The complexity of QAPs is variable, but must ensure the execution of QKD protocol with other quantum equipments such as transmitter, receiver.
- It must use satellite-based QAPs or satellite-based quantum relay station in order to obtain more flexibilities.

In fact, the QCKI is a network, which is named QBONE by us, in which QAPs can be disconnected. The separate QAPs are essential factors of QCKI and their complexity can be different. It means that one party can simply use a transmitter as the one in the first implementation of QKD [5], see figure 6.18 on page 92. But the other party can have the support of a complex

 © Eurocontrol, June 2004.

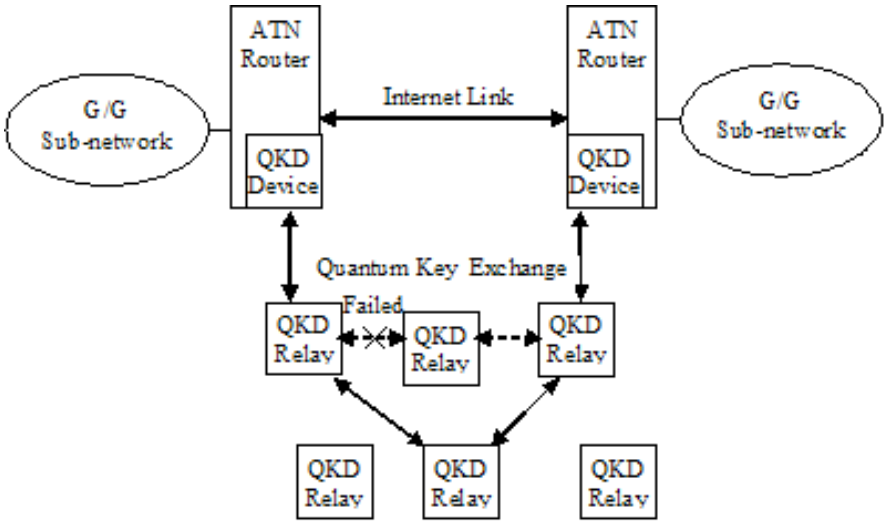


Figure 6.17: QKD relays network and two G/G Subnetworks.

quantum satellite-based network. Therefore, we can incrementally build the QCKI as follows:

- Firstly, we construct independently separate simple ground-based QAPs at several airports. These QAPs can be used immediately to assure the implementation of QKD technology at their airports.
- Then, we can construct fiber-based QKD fixed links which connect several QAPs, which are gateways of the main ATN Sub-networks, for a frequent usage.
- Finally, we can think about the satellites in QCKI in order to have the global QCKI.

With the strategy of incremental construction, we can hope that QCKI will take part soon in ATN Network.

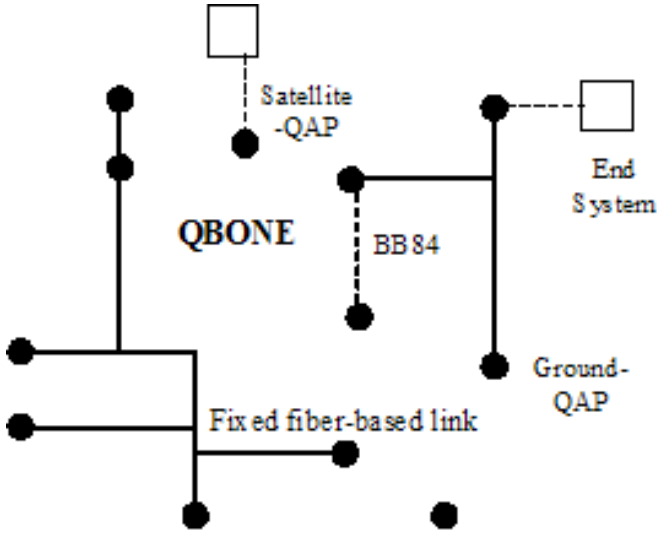


Figure 6.18: The QKCI of ATN Network

 © Eurocontrol, June 2004.

Section 7

QC Communication Protocols

7.1 Introduction to Communication Protocols

According to the preceding sections, we have scenarii for the distribution of a quantum key between an aircraft and a ground station and between other elements of the Aeronautical Telecommunication Network (ATN).

In this part, we develop a secure communication protocol between them. A protocol is the description of all steps from the beginning of the procedure to establish a secured and authenticated communication link between the two parties.

First of all, we can imagine a general protocol which contains three following stages, shown in figure 7.1

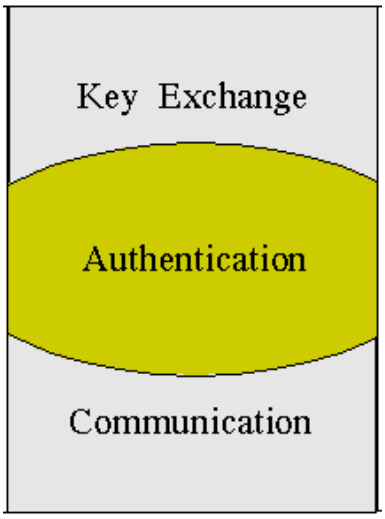


Figure 7.1: Three stages of a general communication protocol.

© Eurocontrol, June 2004.

1. *Secure key exchange using quantum cryptography.* This question is already well described in the preceding sections, cf. section 3 on page 25 for a deep description of the quantum key distribution process.

   We choose to use protocol BB84 to exchange a secure key between the aircraft and the ground station using, for instance, a satellite network. We choose it because it is a simple, well-known et mathematically proved procedure.

   Moreover, we already suggested some physical architectures to distribute the key inside or outside the airport. We also presented models for secure exchange of the quantum key before or after of the aircraft take-off.

2. *Authentication.* Authentication is a procedure to verify that a received message really comes from a certain entity and has not been altered. Authentication is not required in all situation. More precisely, we will see that authentication may be done *by position* in the case of aircrafts instead of using an authentication procedure

3. *Connection establishment.* When one party has obtained the key and has well checked (authenticated) its interlocutor, this party can establish a secure connection for communication using common symmetric encryption mechanism. After a communication period T to be determined, the party go back to the first stage to renew the quantum key.

In the next parts, we will present some authentication protocols. Today, many Quantum Key Distribution (QKD) protocols have been proposed and some have been verified with practical experiments. However, in practice, all the presented QKD protocols are sometimes insecure against the man-in-middle attack because they do not authenticate the parties.

> The *man-in-middle* attack occurs when a legitimate endpoint of the communication link, named Alice, communicates with the other legitimate endpoint of the communication link, named Bob. A third party, named Eve, intercepts all qubits and regular messages sent by Alice to Bob. Then Eve communicates with Bob, impersonating Alice. When Bob answers, Eve intercepts all qubits and regular messages sent by Bob to Alice. Then Eve communicates with Alice, impersonating Bob.
>
> Eve may retransmit the qubits or regular messages without changes. In this case, she is a *passive* eavesdropper.
>
> Or, she may alter the messages to provide false informations. In this case, she is an *active* eavesdropper.

If Eve uses an *active* man-in-the-middle attack during a quantum key establishment session between Alice and Bob, then Eve obtains two keys K_{AE} and K_{EB}. K_{AE} represents the secret quantum key established between Alice and Eve. K_{EB} represents the secret quantum key established between Eve and Bob. As a result Eve can easily decrypt the ciphered texts exchanged between Alice and Bob. If Alice sends a message to Bob, she encrypts the message using the key K_{AE}. Eve intercepts the message, decodes it using K_{AE} and re-encrypts it using K_{EB}. When Bob receives the message, he decodes it using K_{EB}. Eve's interception is similar when Bob sends a message to Alice.

 © Eurocontrol, June 2004.

Thus, it is necessary to check the received messages to ensure that they are not modified, checking *integrity*, and that they really come from the right interlocutor, authentication.

The main point is authentication. If the quantum key exchange is supported with authentication, then the exchanged key is only shared by Alice and Bob and Eve cannot intercept messages.

We can classify authentication algorithms in two groups: classical authentication and quantum authentication. Quantum authentication is currently developed at Enst [40] meanwhile classical authentication technologies are well described in the literature [3].

7.1.1 Classical Authentication

Classical cryptography describes several techniques to implement authentication, i.e. there are several means of realizing authentication [3].

- *Authentication by symmetric-key techniques.* Authentication based on symmetric-key techniques requires the two participants to previously share a key. For a closed system with a restricted number of users, each pair of users may easily share a key. But in larger systems employing symmetric-key techniques, identification protocols often involve the use of a trusted on-line server with which each party shares a key. The on-line server effectively acts like the hub of a spoked wheel providing a common session key to two parties each time one party requests authentication with another party.

  But in the ATN[1], we can use quantum keys, distributed by the protocol BB84, as symmetric authentication keys. Thus, we can solve the problem of shared key using QKD. With this technique, we can apply the methods described below.

  - r_A denotes a random number generated by the participant (party) A using appropriate techniques.
  - E_K denotes a symmetric encryption algorithm such as AES[a], with a key K shared by the two parties.
  - $A \rightarrow B : M$ means that that the participant A sends the message M to the participant B.
  - $A \leftarrow B : M$ means that that the participant B sends the message M to the participant A.
  - Optional message fields are denoted by an asterisk, i.e. "$*$", while a comma, i.e. "," within the scope of E_K denotes concatenation of messages.
  - For sake of concision, Alice may be called A and Bob may be called B.

  [a] Advanced Encryption Standard

[1] Aeronautical Telecommunication Network

1. *Authentication based on symmetric-key encryption.* In this case, the two parties (the participants A and B) may carry out unilateral entity authentication in two passes using random numbers. This authentication algorithm is described as follows.

$$A \leftarrow B \quad : \quad r_B \tag{7.1}$$
$$A \rightarrow B \quad : \quad E_K(r_A, r_B, B^*) \tag{7.2}$$
$$A \leftarrow B \quad : \quad E_K(r_A, r_B) \tag{7.3}$$

   where K is the shared key. Upon reception of message (7.2), B carries out checks as above and, in addition, recovers the decrypted r_A for inclusion in (7.3). Upon decrypting (7.3), A checks that both random numbers match those used earlier.

2. *Authentication based on one-way function.* One-way functions are similar to hash functions. Providing arguments, they can fastly compute a result but they are not reversible: providing the result, it is impossible to recover the argument. Cryptographic researchers have defined indexed families of one-way function. Providing a key K, we name h_K the one-way function indexed by K.

   This method is similar to above mechanism but symmetric encryption algorithm E_K is replaced by a one-way or non-reversible function h_K indexed by the previously shared key K:

$$A \leftarrow B \quad : \quad r_B \tag{7.4}$$
$$A \rightarrow B \quad : \quad r_A, h_K(r_A, r_B, B) \tag{7.5}$$
$$A \leftarrow B \quad : \quad h_K(r_A, r_B, A) \tag{7.6}$$

- *Authentication by public-key techniques.* Public-key techniques may be used for authentication based identification.

  Each participant has a public key known by every other participant and even known by the eavesdropper. The public key allows to encrypt messages. But decryption is only possible with the private key which is only known by the participant.

  In public key technique, a participant demonstrates the knowledge of its private key without disclosing it. Because the participant is the only one knowing its private key, this is a sure identification. This can be done in one of the two following ways.

  1. *Authentication based on public-key decryption.*

     - P_A and P_B denote the public key encryption algorithms of participants A and B.
     - h is a one-way hash function.
     - r_A and r_B denote random numbers produced by A and B.

     Consider the following protocol:

$$A \rightarrow B \quad : \quad h(r_A), P_B(r_A, A) \tag{7.7}$$
$$A \leftarrow B \quad : \quad h(r_B), P_A(r_A, r_B) \tag{7.8}$$
$$A \rightarrow B \quad : \quad r_B \tag{7.9}$$

     A chooses a random r_A, computes the witness $x_A = h(r_A)$ and the challenge $e_A = P_B(r_A, A)$. A sends (7.7) to B. B decrypts e_A to

 © Eurocontrol, June 2004.

recover r'_A and A', computes $x'_A = h(r'_A)$. B quits if $x'_A \neq x_A$, implying $r'_A \neq r_A$. Otherwise, B chooses a random r_B, computes $x_B = h(r_B)$ and $e_B = P_A(r_A, r_B)$. B sends (7.8 on the facing page) to A. A decrypts e_B to recover r'_A and r'_B, computes $x'_B = h(r'_B)$. B quits if $x'_B \neq x_B$. Otherwise, if $r'_A = r_A$, B is well authenticated, and A sends $r_B = r'_B$ to B. B succeeds with entity authentication of A upon verifying the received r_B.

2. *Authentication based on digital signatures.* This way is a strong authentication protocol specifying identification based on digital signatures and, respectively, time-stamps and random number challenge.

   - r_A and t_A denote a random number and a times-tamp generated by A.
   - S_A denotes the signature mechanism of A.
   - $cert_A$ denotes the public-key certificate of A.

   Here follows mutual authentication with random number:

$$A \leftarrow B \quad : \quad r_B \tag{7.10}$$
$$A \rightarrow B \quad : \quad cert_A, r_A, B, S_A(r_A, r_B, B) \tag{7.11}$$
$$A \leftarrow B \quad : \quad cert_B, A, S_B(r_A, r_B, A) \tag{7.12}$$

   B verifies that the clear-text identifier is its own identifier. Then using a valid signature public key for A, i.e. $cert_A$, it verifies that A's signature valid over the clear-text random number r_A, the same number r_B as sent in (7.10), and this identifier. And (7.12) is processed analogously to (7.11).

Analysis 7.1.1. *In these classical methods, there are two ways to verify identifiers of participants: authentication by symmetric-key techniques and authentication by asymmetric-key techniques (public-key techniques). With first method, we can use quantum key as a shared key in symmetric encryption algorithm. And in second, we can integrate PKI[2] into QKD[3] to solve problem of authentication.*

7.1.2 Quantum Authentication

Quantum authentication is a process to verify identifiers of legitimate users in key exchange using protocols similar to QKD protocol. This method uses as well a secret key (authentication key) to authenticate but be safe against the man-in-middle attack and the *Denial of Service* (DoS) attack.

The DoS (Denial of Service) attack is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. In the case of authentication, a typical DoS attack consists for a false participant to repeatedly trying to authenticate himself. At each try, the true participant uses a new pre-positioned key. If it does not use a new key each time, the false participant may gain a few information on the key at each try. If a new key is used at each try, the set of pre-positioned key can be exhausted.

[2]Public Key Infrastructure
[3]Quantum Key Distribution

The Quantum Authentication protocol, developed by our team at Enst, is described in the following section. It is safe against man-in-the-middle attack and against the Denial of Service (DoS) attack.

7.2 Quantum Authentication Protocol

In this party, we present a quantum authentication protocol [21, 40]. This authentication scheme is based on the same technique as the BB84 protocol. Here we assume A and B are two participants who want to authenticate themselves.

Let m be a message and let k be a key. m and k are supposed to have the same bit-length. The Vernam encryption of m using key k is written $m \oplus k$. It is an XOR, or equivalently an addition modulo 2, of the corresponding bits of m and k, i.e. if m_i is the i-th bit of m, if k_i is the i-th bit of k, then the i-th bit of $m \oplus k$ is m_i XOR b_i.

Given the encrypted message $m \oplus k$ et the key k, the message can be recovered by computing $(m \oplus k) \oplus k$.

Using the theory of Information of Shannon, it can be proved that Vernam cipher is uncontionnally secure provided that the keys are used only once.

A and B use a shared authentication key as precedently described. Let us name k this key of bit-length n.

- $k \uparrow$ and $k \downarrow$ respectively denote the string $k = (k[1], ..., k[n])$ and its inverse $(k[n], ..., k[1])$.
- Let m a message of length $p \cdot n$, $m \oplus k$ denotes the Vernam encryption of message m by a key obtained by concatenating p copies of the key k.

The protocol executes the following steps. The terminology can be found in section 3 on page 25 describing the BB84 protocol.

1. A generates a random bit string.
2. For presenting each bit, and uses a quantum eigen state in a random basis chosen in $\{\oplus, \otimes\}$.
3. A sends these quantum states to B.
4. B uses a random basis chosen in $\{\oplus, \otimes\}$ to measure each received quantum state.
5. The bases used by A for quantum encoding are collected into a bit string b_a: 0 for $\oplus$, 1 for $\otimes$.
6. A encrypts the string b_a with the pre-positioning key $k \downarrow$ and sends the string $(b_b \oplus k \downarrow)$ to B using the classical public channel.

 © Eurocontrol, June 2004.

7. The bases used by B for quantum measurements are collected into a bit string b_b: 0 for $\oplus$, 1 for $\otimes$.
8. B encrypts the string b_b with the pre-positioning key $k \uparrow$ and sends the string $(b_b \oplus k \uparrow)$ to A using the classical public channel.
9. A and B decrypt the bases received and could then find out $b_a \oplus b_b$.
10. They discard the results at all positions i where $b_a[i] \oplus b_b[i] = 1$, i.e. positions where $b_a[i]$ and $b_b[i]$ are different. They interpret the rest and get the two strings x_a for A and x_b for B.
11. A and B can compare some distilled bits from x_a and x_b to detect the presence of Eve, the eavesdropper impersonating the parties.
12. If Eve is not detected, then they validate the authentication.

Security Analysis

We only give informal deduction. Full quantum-based et information theory-based proof are currently built.

- *Against passive attacks.*

  This scheme would more secure than BB84 where b_b is transfered in plain-text.

- *Against active attacks.*

  - *Against the man-in-middle attack.*

    For the case Eve impersonates B to communicate with A.

    She would use a random key k_e and sends $(b_e \oplus k_e)$ to A.

    A considers $(b_e \oplus k_e)$ as sent by B. A calculates $b_b = b_e \oplus k_e \oplus k \uparrow$ and announces $(b_a \oplus k \downarrow)$ to Eve. A would maintain the result at positions i where $b_a[i] \oplus b_b[i] = 0$.

    Therefore, the positions i are not announced to Eve, and she cannot calculate i from $(b_a \oplus k \downarrow)$, k_e and b_e. She would deduce x_e from the measurement result at some random position i'.

    Thus, x_a and x_e are of different lengths and independent. And if A and Eve compare some distilled bits from x_a and x_e, there would be an average error rate of 50% that would be detected.

  - *Against the DoS attack.*

    For the case Eve impersonates B to communicate with A.

    As Eve does not know if the bit code for the i-th quantum state corresponding to $b_a[i]$ is maintained or not, she does not know either which bits are in x_a.

    We could estimate that the uncertainty about measurement of new key bit is bound by $H(k \downarrow \oplus k \uparrow)$ where H is the entropy function of Shannon.

    Thus, he could not use A's announcement of some distilled bits from x_a to discover the corresponding bases used by A and he could not gain information about the authentication key $k \downarrow$ or $k \uparrow$.

7.3 Communication protocols

With the models of key exchange and authentication, we can set up a secure connection. There are two communication protocols proposed corresponding to quantum authentication protocol, or to the classical authentication protocols: authentication by symmetric-key protocol or authentication by public-key techniques.

1. *Communication protocol with quantum authentication.*

   This protocol is also applied to authentication by symmetric-key protocol.

   In this model, we use a shared key previously exchanged in a first stage. This key is a quantum key k of n random bits, in case of quantum authentication, or as a shared key in the case of symmetric authentication.

   After checking the participants (authentication) in a second stage, we pass to a third stage to establishing a secure connection with shared key exchange in first stage as shown in figure 7.2 on the next page.

2. *Communication protocol with authentication by public-key techniques.*

   In this method, we integrate asymmetric cryptography to this model.

   In stage of authentication, we use a public and private key pair to authenticate. Because the two stages (1) and (2) are independent, we use a certified message ciphered by two secret keys $cert_1$ and $cert_2$: one is the quantum key distributed in the first stage (1), the other is the private key of second stage (2).

   We cancel the operation to establish a connection and repeat to first stage if $cert_1 \neq cert_2$. Otherwise, we set up a secure connection with quantum key, as shown in figure 7.3 on the facing page.

In short, we can apply both protocols. The first protocol with the quantum authentication, it is simpler, it is safe and it can prevent the man-in-middle attack and DoS attack. The second is more complex but it is also protected because two stages of key exchange and of authentication are independent.

 © Eurocontrol, June 2004.

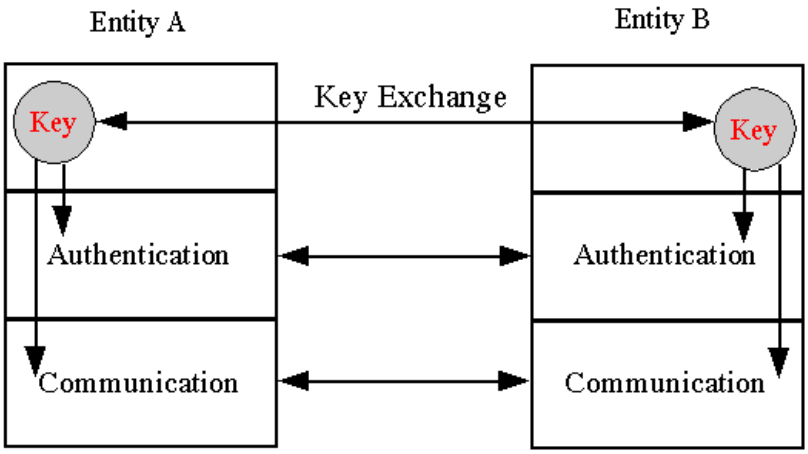


Figure 7.2: Communication with symmetric or quantum authentication.

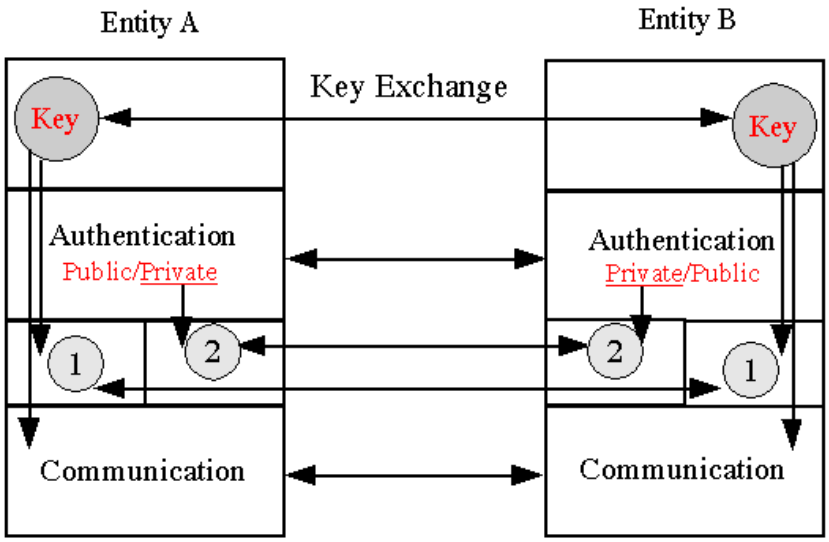


Figure 7.3: Communication protocol with asymmetric authentication.

WP III

Visual Demonstrators

© Eurocontrol, June 2004.

Summary and Conclusions

This part summarizes the conclusions of the third step of this study. These conclusions are made explicit in the following sections.

Summary

- Chapter 8 on page 107, *"AIT/QKD Animations in Flash"*, is a description of the five Flash animation explaining the coupling of AIT and QKD.
- Chapter 9 on page 113, *"BB84 Demonstrator in Java"*, is the documentation for using the BB84 Java demonstrator which illustrates a session of Quantum Key Distribution.

© Eurocontrol, June 2004.

Section 8

AIT/QKD Animations in Flash

In this section, we present animations in Flash to visualize theorys in the preceding sections.

8.1 Installation

These demonstrations are written in Flash, therefore it is easy to intall.

First, unzip the file `AITQKD_anims.zip`. You normally get a directory `AITQKD_anims` containing several files.

You can copy these files:

- `ait.html`, `ait.swf`, `ait_qkd.html`, `ait_qkd.swf`, `atn.html`, `atn.swf`, `flightplan.html`, `flightplan.swf`, `index.html`, `intro.html`, `menu.html`, `qkd.html`, `qkd.swf`

in a same directory wherever you want.

These files may be be installed on a WEB server if you want to make the demo publicly available.

8.2 Opening `index.html`

To see the demo, you must open the file `index.html` in a navigator that has the Flash plugin installed.

Shown in figure 8.1 on page 109, you can see the principal interface. There are 5 features which we will explain in the following parts.

© Eurocontrol, June 2004.

8.3 Air Identification Tag - AIT

Click on **1. AIT**.

This animation, show in figure 8.2 on the facing page, demonstrate the AIT, *show in section 2.6 on page 23 "Air Identification Tag"*, and also the risks of this communication, *show in section 1.1 on page 11 "Why Security?"*.

AIT aims at improving and facilitating identification. IT inserts automatically an unnoticeable small data-link channel in the communication. The inserted data can be a digital signature associated with the emitter and may be used to achieve reinforcement of audible stimulus with a visual stimulus. But this communication method is opposite the attacks: *monitoring, spoofing, modifying*. Therefore, one needs the ways coded with the quantum key, show in following section.

8.4 Quantum Key Distribution

Click on **2. QKD**.

To securely communicate, the plane and the control stations must have the same key coding. For that, before taking off, the plane is distributed a key by the tower control, *show in figure 8.3 on page 110, show also in section 3.3 on page 29 "Quantum Key Distribution" and in section 6.2 on page 78 "Scenario of QKD in ATN"*

8.5 Flight plan and ATN

Click on **3. Flight plan** and then on **4. ATN**.

After the distribution the key to the aircraft, this key is dispatched to all station where the plane will pass, *show in figure 8.4 on page 110*. There are two ways distributing the key between the stations: distribution by a satellite network, *show in section 5 on page 57*, or direct distribution that depends the distance between them. In this demonstration, we visualize a direct scenario, *show in figure 8.5 on page 111*

8.6 Authentication and Integrity

Click on **AIT + QKD**.

On board, the plane can communicate with the stations on its plan with the authentication by using the distributed key, *show in figure 8.6 on page 111*

 © Eurocontrol, June 2004.

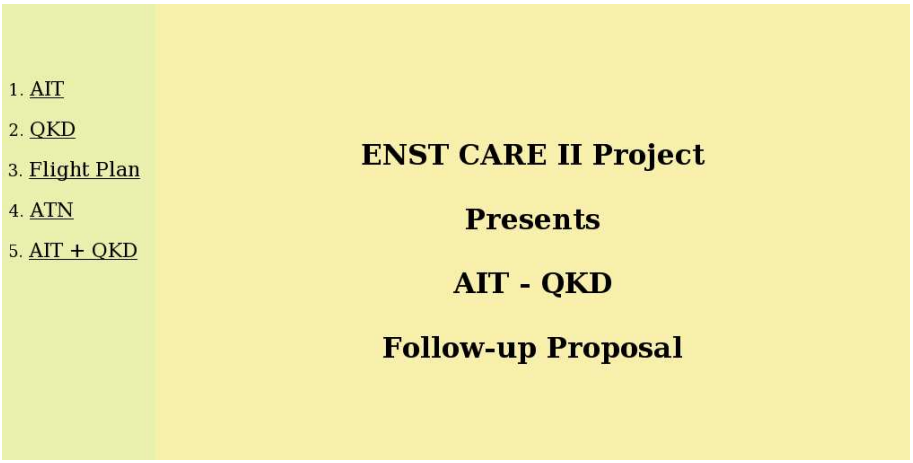


Figure 8.1: Demonstration in Flash

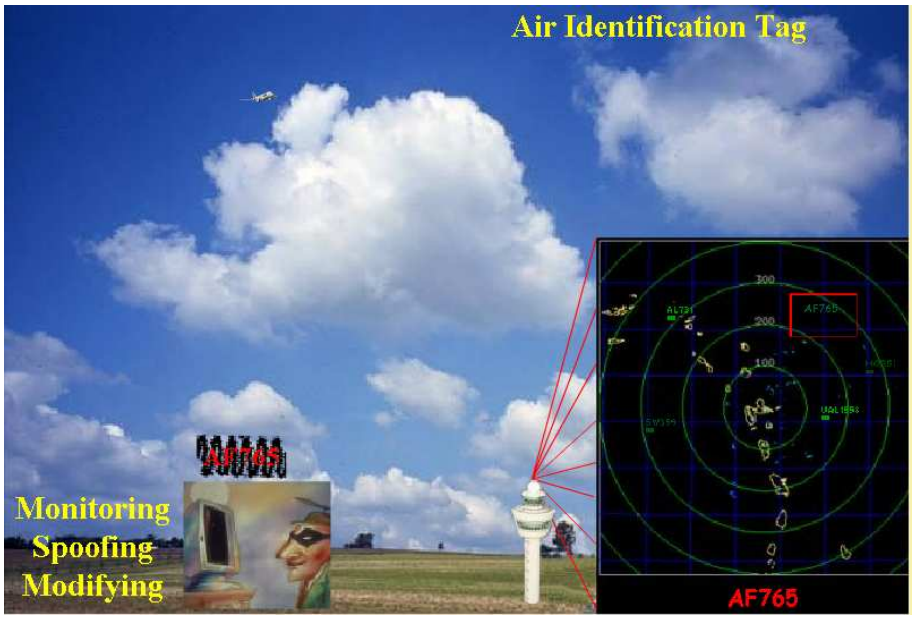


Figure 8.2: Air Identification Tag

Figure 8.3: Quantum Key Distribution

Figure 8.4: Flight Plan

 © Eurocontrol, June 2004.

Figure 8.5: ATN: Key Dispatching

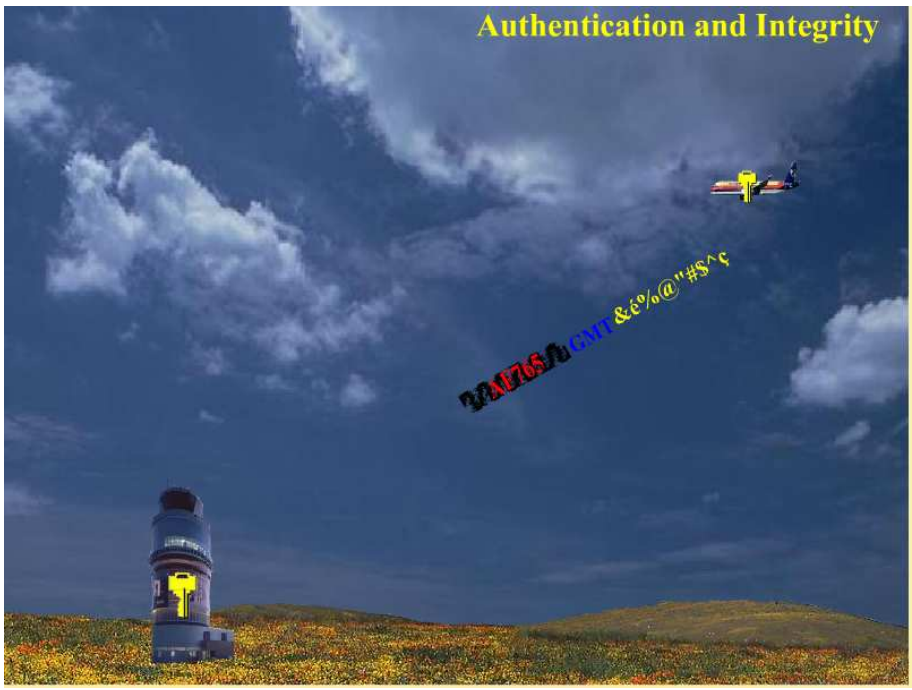


Figure 8.6: Authentication and Integrity

Section 9

BB84 Demonstrator in Java

User Manual

Following chapter 3 on page 25, the QKD simulator is composed of six packages, including 23 source files, 6 executable jar files and a Makefile. This program is compatible with Unix, Linux, MacOS and Windows.

9.1 Program installation

Choose and follow the suitable guide with your operating system. Verify that **jdk1.4.0** or later or the equivalent **jre** is installed on yourmachine.

Unpack the file `BB84_demo.zip` to obtain the directory `BB84_Protocol`.

9.1.1 For users on Unix, Linux or MacOS

To unpack `BB84_demo.zip`, type on the command line:
`unzip BB84_demo.zip`

On MacOS systems, you can double-click on the file `BB84_demo.zip`.

After execution of this command, you have a directory named `BB84_Protocol`. And there you can find sources, executalbe files, and the simulation api specification.

Recompiling the files is not necessary, but if you want to recompile all the programs, you need the **jdk**:

- To remove all already compiled classes, use command:
  `make clean`
- To compile source files to obtain classes, run command:
  `make`

© Eurocontrol, June 2004.

9.1.2 For users on Windows

Using a compression utility to unpack the file `BB84_demo.zip`, such as WinZip, WinRar or Total commander...

If your Windows is well configured, it may be sufficient to double-click on `BB84_demo.zip`.

Recompiling the files is not necessary but once obtaining directory `BB84_Protocol`, you can do the same as users of MacOS, Linux or Unix to recompile the program using command line.

In the case of being unfamiliar with command, you can use an editor supporting java language to recompile sources or run Makefile.

9.2 How to run simulator

To run the program, enter BB84_Protocol directory...

9.2.1 For users on Unix, Linux or MacOS

To launch the simulator, typing command on a command line: `make run`

or click directly on jar files `alice.jar`, `bob.jar`, `eve.jar`, `qc.jar`, `pc.jar` in current directory in the file manager window

9.2.2 For users on Windows

You can do the same as users of MacOS, Linux or Unix to run the program on command-line.

Or if you are familiar with Windows Explorer, launch the simulator by click on five executable files in the current directory: `alice.jar`, `bob.jar`, `eve.jar`, `qc.jar`, `pc.jar`

9.2.3 The application is running

.

Five windows will be displayed on your screen.

Once the simulator is launched, you will see five windows laid out on the screen with the appropriate title: *Alice*, *Bob*, *Eve*, *Quantum Channel* and *Public Channel*.

And now you get a screen as below:

All the control buttons are on windows *Alice* and *Bob*. After the configuration of all parameters on window *Alice*, *Eve* and *Quantum Channel*, you can start the transmission of photons on the quantum channel from *Alice* to *Bob*

 © Eurocontrol, June 2004.

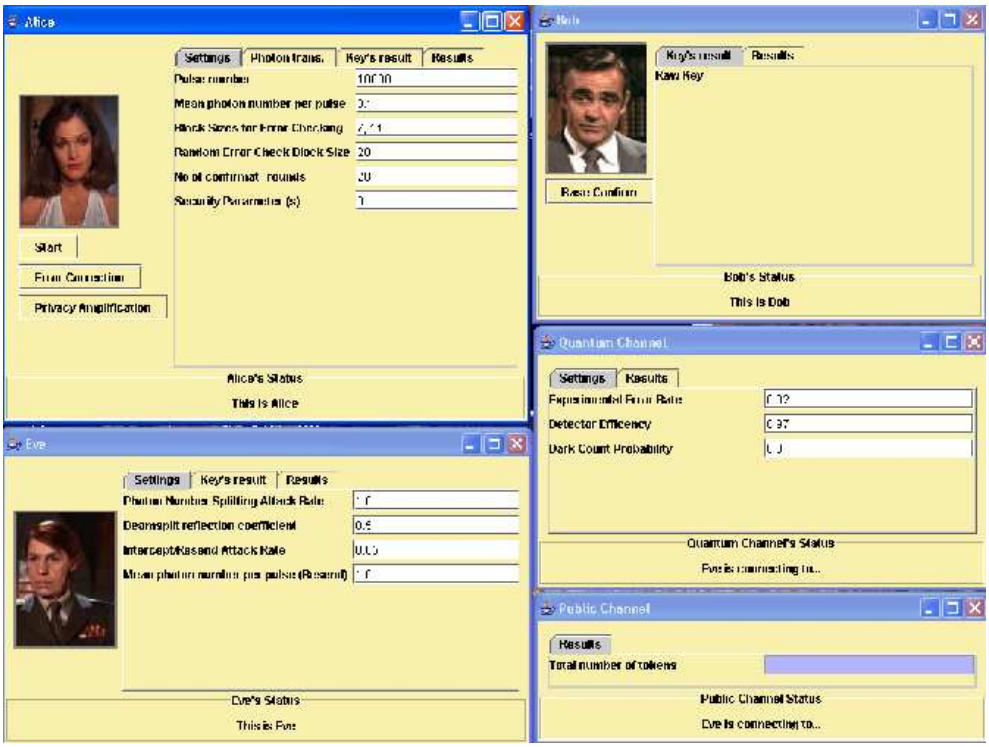


Figure 9.1: Alice's setting window

by click on button **Start** on *Alice* window. This process is observed on *Photon Transmission* tab.

After transmission finished, total number of photons detected by Bob will be displayed on the *Result* tab of *Quantum Channel*. Besides, you can know the number of errors made in this channel due to configured experimental error rate on the *Settings* tab, and also the number dark counts detected.

Now pass to phase Base Confirm on press the button **Base Confirm** of the same name on *Bob* window, and the result *Raw Key* is produced.

On the panel, you may see some green bits on both *Alice* and *Bob* panels at these positions bases used are not correlated. And below are the bits in *Raw Key* which Eve eavesdropped.

Now you realise sequentially phases **Error Correction** and **Privacy Amplification** by pressint the relative buttons in *Alice* window. Note the status of each panel to choose the correspond button. Sometimes, in phase error correction, there may be not enough bits to check errors, so the protocol will be restarted by clicking **Start** again on *Alice* panel.

When the text *Finished* is displayed on all status bars, it is the moment the protocol is completed. The final key may be produced or not in the case there had not been enough bits in phase of error correction.

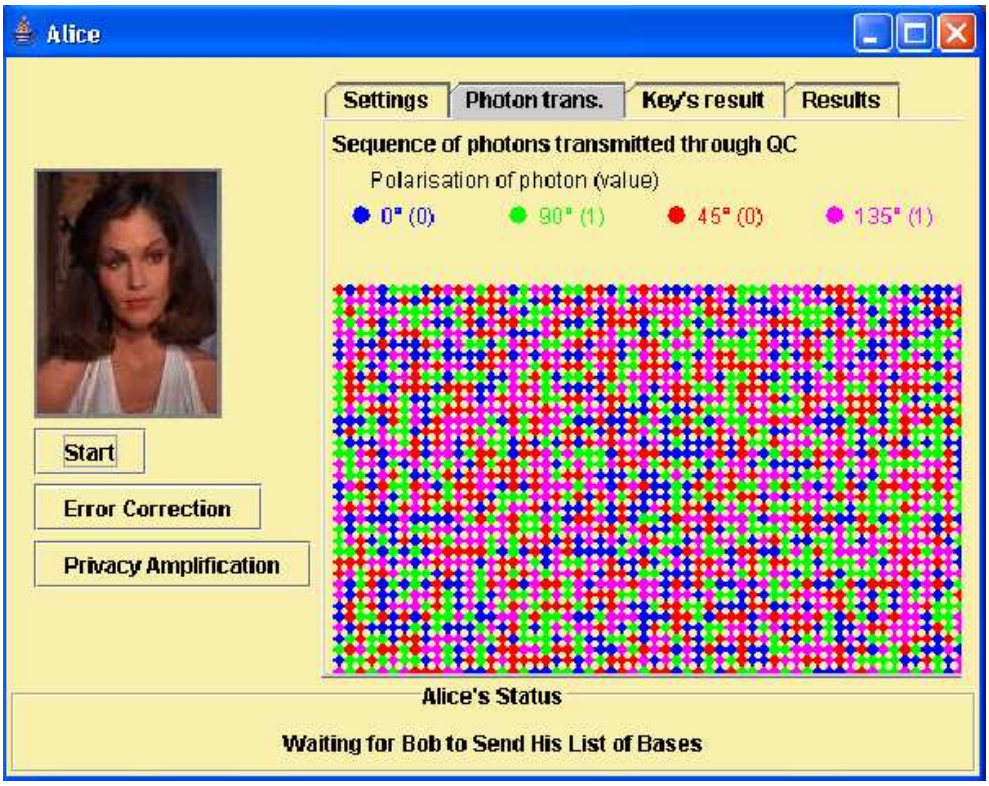


Figure 9.2: Process of photons transmission

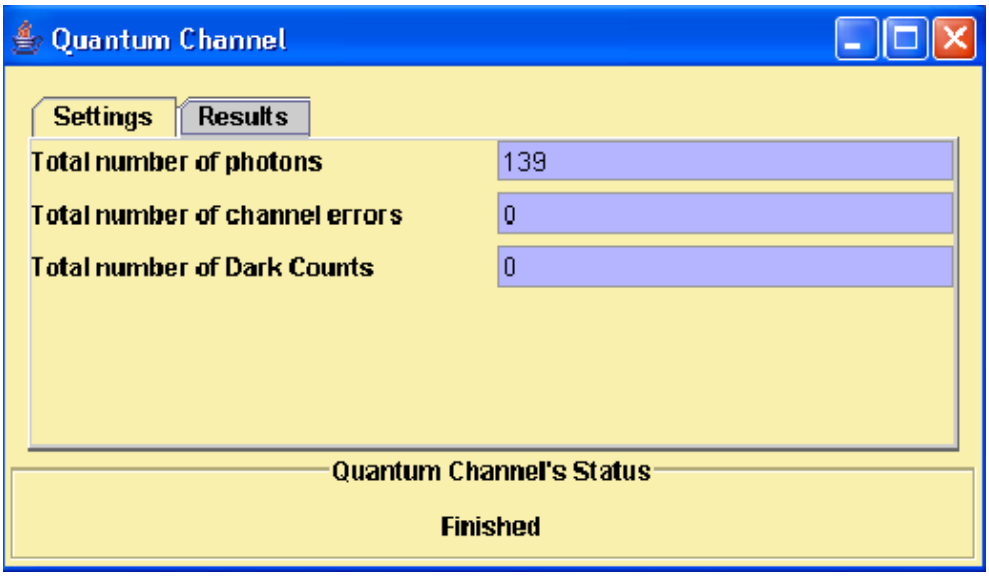


Figure 9.3: Quantum Channel's result window

 © Eurocontrol, June 2004.

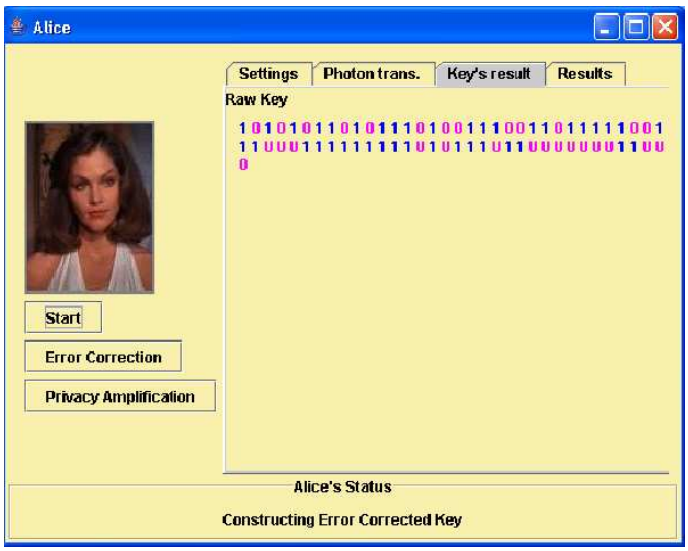


Figure 9.4: Alice's Raw key

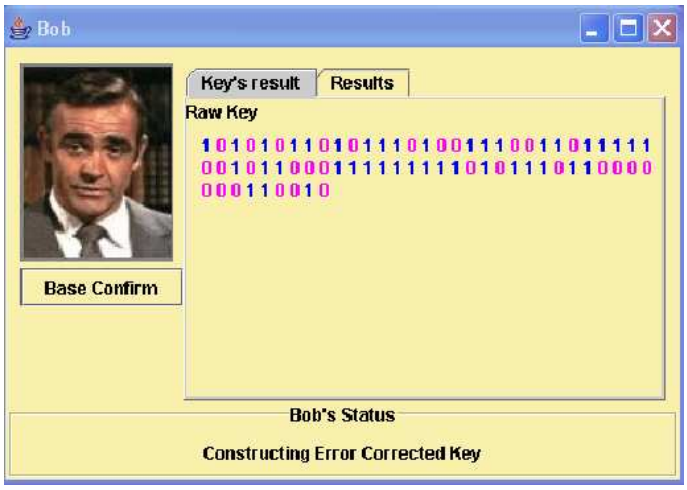


Figure 9.5: Bob's Raw key

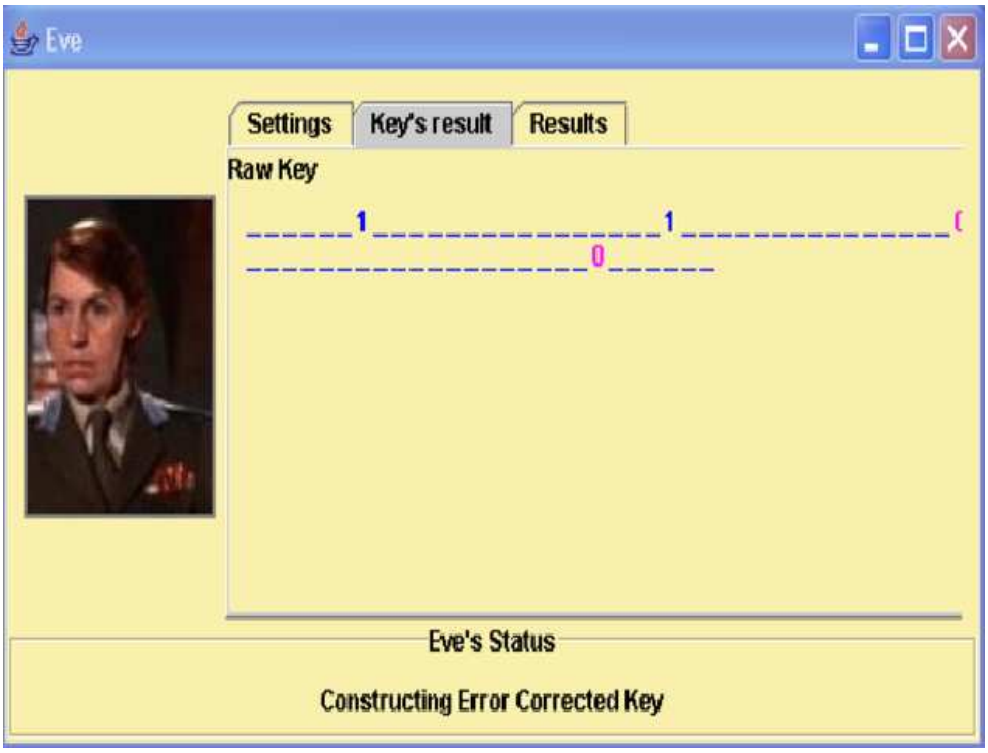


Figure 9.6: Eve's Raw key

Figure 9.7: Result of Error Correction

 © Eurocontrol, June 2004.

Figure 9.8: Result of Privacy Amplification

Acronyms

A/G	Air/Ground
AAC	Aeronautical Administrative Communications
AAIM	Aircraft Autonomous Integrity Monitoring
ABAS	Airborne Based Augmentation System
ACARS	Aircraft Communications Addressing and Reporting System
ACAS	Airborne Collision Avoidance System
ACC	Area Control Centre
ACSE	Association Control Service Element
ADLP	Aircraft Data Link Processor
ADS	Automatic Dependent Surveillance
ADS-B	Automatic Dependent Surveillance - Broadcast
ADSP	Automatic Dependent Surveillance Panel
AEEC	Airlines Electronic Engineering Committee
AES	Airborne End System
AF	Auto-Forward
AFC	Area Forecast Centre
AFCAC	African Civil Aviation Conference
AFS	Aeronautical Fixed Service
AFTN	Aeronautical Fixed Telecommunications Network
AGT	Air-Ground Telecommunication
AIDC	ATS Interfacility Data Communication
AINSC	Aeronautical Industry Service Communication
AIP	Aeronautical Information Publication
AIR	Aeronautical Information Region
AIS	Aeronautical Information Service
AISC	Aeronautical Industry Service Communication
AIT	Air Identification Tag
ALLPIRG	All Planning and Implementation Regional Groups
AM	Mobile DTE Sub-Address
AMCP	Aeronautical Mobile Communication Panel
AMHS	Aeronautical Message Handling System
AMSS	Aeronautical Mobile Satellite Service
ANC	Air Navigation Commission
ANP	Air Navigation Plan
ANS	Air Navigation Services
AOC	Aeronautical Operational Control
AP	Application Process
APANPIRG	Asia Pacific Air Navigation Planning and Implementation Regional Group
APC	Aeronautical Passenger Communications
APIM	ARINC IA Project Initiation/Modification

© Eurocontrol, June 2004.

APIRG	Africa-Indian Ocean Planning and Implementation Regional Group
APP	Approach
ARINC	Aeronautical Radio Inc.
ARTAS	ATS Radar Tracker and Server
ASECNA	African States Association
ASEs	Application Service Elements
ASM	Airspace Management
ASN.1	Abstract Syntax Notation No. 1
ASPP	Aeronautical Fixed Service and System Planning Panel
ATAG	Air Transport Action Group
ATC	Air Traffic Control
ATCAA	Air Traffic Control Assigned Airspace
ATFM	Air Traffic Flow Management
ATM	Air Traffic Management
ATM	Asynchronous Transfer Mode
ATN	Aeronautical Telecommunication Network
ATNP	ATN Panel
ATNSI	ATN Systems Inc.
ATS	Air Traffic Services
ATSC	Air Traffic Services Communications
ATSU	Air Traffic Service Unit
AWOP	All Weather Operations Panel
BIS	Boundary Intermediate System
BNS	Basic Name Server
CA	Certification Authority
CAA	Civil Aviation Authority
CAERAF	Common American European Reference ATN Facility
CARD	CNS/ATM Research and Development
CASITAF	CNS/ATM Systems Implementation Task Force
CATC	Civil Aviation Training Centre
CBA	Cost Benefit Analysis
CCITT	Comité Consultatif International Télégraphique et Téléphonique
CDC	Consistent Data Store
CDTI	Cockpit Display of Traffic Information
CEC	Commission of the European Communities
CIDIN	Common ICAO Data Interchange Network
CLNP	Connectionless Network Protocol
CLNS	Connectionless Network Service
CLTP	Connectionless Transport Protocol
CM	Context Management
CMA	Context Management Application
CMU	Communications Management Unit
CNS	Communications, Navigation and Surveillance
CNS/ATM	CNS/Air Traffic Management
CNS/ATM-1	CNS/ATM Package 1
CNSI	CNS Implementation
COCESNA	Carribbean and Central American States Association
COG	Co-ordination Group
COTP	Connection Oriented Transport Protocol
COTS	Connection-Oriented Transport Service

 © Eurocontrol, June 2004.

CPDLC	Controller-Pilot Data Link Communications
CRL	Certificates Revocation List
CSMA	Carrier Sense Multiple Access
CTS	Conformance Test Suite
CWP	Controller Working Position
D8PSK	Differentially encoded 8-Phase Shift Keying
DAC	Dual Attached Concentrator
DAS	Dual Attached Station
DES	Data Encryption Standard
DOS	Denial Of Service
DLK	Data LinK
DME	Distance Measuring Equipment
DSP	Data link Service Provider
DTE	Data Terminal Equipment
EANPG	European Air Navigation Planning Group
EATCHIP	European ATC Harmonisation and Integration Programme
EATMS	European Air Traffic Management System
ECDSA	Elliptic Curve Digital Signature encryption Algorithm
ECAC	European Civil Aviation Conference
ECU	European Currency Unit
EDP	Entanglement Distillation Protocols
EGNOS	European Geostationary Navigation Overlay System
ELM	Extended Length Message
EOLIA	European preOperational dataLInk Applications
ERD	End Routing Domains
ES	End System
ESCAN	Electronically Scanned
EUR	Europe
EUROCONTROL	European Organisation for the Safety of the Air Navigation
FAA	Federal Aviation Administration
FANS	Future Air Navigation System
FASID	Facilities and Systems Implementation Document
FDDI	Fibre Distributed Data Interface
FDMA	Frequency Division Multiple Access
FIC	Flight Information Centre
FIFO	First In First Out
FIR	Flight Information Region
FIS	Flight Information Services
FL	Flight Level
FMS	Flight Management System
FPL	Filed Flight Plan
FUA	Flexible Use of Airspace
G/G	Ground/Ground
GA	General Aviation
GBAS	Ground Based Augmentation System
GDLP	Ground Data Link Processor
GEO	GEOstationary orbit
GES	Ground Earth Station

GICB	Ground Initiated Comm-B
GLONASS	Global'naya Navigatsionnaya Sputnikovaya Sistema
GM	Guidance Material
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GREPECAS	Caribbean/South American Regional Planning and Implementation Group
GS	Ground Station
GULS	ISO Generic Upper Layer Services
HF	High Frequency (3-30 MHz)
HMAC	Hybrid symmetric, Hashed Message Authentication Code
HMI	Human Machine Interface
HR	Human Resources
IA	Interconnection Agreement
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
ICC	Inter-Centre Co-ordination
ICC	Inter-Centre Communications
IDRP	Inter-Domain Routing Protocol
IEC	International Electrotechnical Committee
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFALPA	International Federation of Airline Pilots' Associations
IFATCA	International Federation of Air Traffic Controllers Associations
IFR	Instrument Flight Rules
II	Interrogator Identifier
ILS	Instrument Landing System
IMC	Instrument Meteorological Conditions
IMG	Implementation Management Group
INS	Inertial Navigation System
IOC	Input/Output Calls
IP	Internet Protocol
IPC	Inter Process Communication
IPR	Intellectual Property Rights
IRDP	Inter-Domain Routing Protocol
IRS	Inertial Reference System
IS	Intermediate System
ISDN	Integrated Services Digital Network
ISO	International Standards Organisation
ITU	International Telecommunications Union
JAA	Joint Aviation Authorities
Kb	K bytes = 1024 bytes
LAAS	Local Area Augmentation System
LAN	Local Area Network
LAP	Link Access Protocol
LAP-B	Link Access Protocol Type B
LE	Link Establishment
LEOs	Low Earth Orbit Satellites

 © Eurocontrol, June 2004.

LLC	Logical Link Control
LREF	Local Reference
LTEP	Legal and Technical Experts Panel
MAC	Media Access Control
MAP	Meteo Aeronautical Charts
MASPS	Minimum Aviation System Performance Standards
MEOs	Medium Earth Orbit Satellites
MET	Meteorological
METAR	Meteorological Aerodrome Report
MHS	Message Handling System
MIDANPIRG	Middle East Air Navigation Planning And Implementation Regional Group
MLS	Microwave Landing System
MMR	Multi-Mode Receiver
MNPS	Minimum Navigation Performance Specification
MSAS	Multi Purpose Satellite Based Augmentation System
MTSAT	Multi Purpose Transport Satellite
MWO	Meteorological Watch Offices
Mode S SSR	Mode S Secondary Surveillance Radar
NAMPG	North American Planning Group
NAS	National Airspace System
NAT	North Atlantic
NAT	Network Adress Translator (*Internet*)
NATIMG	North Atlantic Implementation Management Group
NATSPG	North Atlantic Systems Planning Group
NAV	Navigation
NDB	Non Directional Beacon
NM	Nautical Mile
NOTAM	Notice to Airmen
NPDU	Network Protocol Data Unit
NPM	Node and Process Management
NPV	Net Present Value
NSAP	Network Service Access Point
OACA	Operating Agency Certificate Authority
OCD	Operational Concept Document
ODIAC	Operational Development of Initial Air/Ground Data Link Communications
OF	Option Flag
OPMET	Operational Meteorological Traffic
ORD	Operational Requirements Document
OSI	Open Systems Interconnection
PAC	Pacific
PAT	Pointing Acquisition and Tracking
PANS	Procedures for Air Navigation Services
PAR	Precision Approach Radar
PDC	Private Data Channel
PDU	Protocol Data Unit
PER	Packed Encoding Rules
PETAL	Preliminary Eurocontrol Test of Air/ground data Link
PIRG	Planning and Implementation Regional Group

PIT	PETAL Integration Team
PKI	Public Key Infrastructure
PSR	Primary Surveillance Radar
QAP	Quantum Access Point
QBER	Quantum Bit Error Bit
QBONE	Quantum Bone
QC	Quantum Cryptography
QCKI	Quantum Confidentiality Key Infrastructure
QKD	Quantum Key Distribution
QoS	Quality of Service
QUBIT	QUantum BIT
RA	Resolution Advisory
RAC	Rules of the Air and Air Traffic Services
RAF	Reference ATN Facility
RAFC	Regional Area Forecast Centre
RAIM	Receiver Autonomous Integrity Monitoring
RCP	Required Communications Performance
RD	Routing Domain
RDT	Research, Development and Test
RF	Radio Frequency
RFC	Request for Comments
RFI	Radio Frequency Interference
RGCSP	Review of the General Concept of Separation Panel
RMCDE	Radar Message Conversion and Distribution Equipment
RNAV	Area Navigation
RNC	Required Navigation Capability
RNP	Required Navigation Performance
RNPC	Required Navigation Performance Capability
RRI	Router Reference Implementation
RSP	Required System Performance
RTCA	Radio Technical Commission for Aeronautics
RTSP	Required Total System Performance
RVSM	Reduced Vertical Separation Minima
SAC	Single Attached Concentrator
SARPS	Standards and Recommended Practices
SARPs	Standards and Recommended Practices
SAS	Single Attached Station
SBAS	Space Based Augmentation System
SCM	System Control and Monitoring
SICAS	SSR Improvements and Collision Avoidance Systems
SIGMET	Significant Meteorological Effects
SIGWX	Significant Weather
SIR	Serveur d'Informations Radar
SISCASP	Secondary Surveillance Radar Improvements and Collision Avoidance Systems
SLM	Standard Length Message
SMGCS	Surface Movement Guidance and Control System
SNDCF	Subnetwork Dependent Convergence Function
SO	Specialist Objective
SPG	Spectrum Protection Group
SSR	Secondary Surveillance Radar
STDMA	Self-Organising Time Division Multiple Access

 © Eurocontrol, June 2004.

STP	Standardized Training Package
SUA	Special Use Airspace
SVC	Switched Virtual Circuit
TAF	Terminal Area Forecast
TAR	Trials ATN Router
TC	Temporary Channel (counter)
TC	Transport Connection
TCAS	Traffic Alert/Collision Avoidance System
TCB	Technical Co-operation Bureau
TCDC	Technical Co-operation amongst Developing Countries
TCM	Time and Clock Management
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TDWR	Terminal Doppler Weather Radar
TFM	Traffic Flow Management
TIS	Terminal Information Services
TIS	Traffic Information Service
TLS	Target Level of Safety
TMA	Terminal Manoeuvring Area
TPDU	Transport Protocol Data Unit
TRD	Transit Routing Domains
TS	Transport Service
TSDU	Transport Service Data Unit
UAL	Upper Layer Architecture
UBSS	Unix Basic System Software
UDP	User Datagram Protocol
ULA	Upper Layer Architecture
UNDP	United Nations Development Programme
USA	United States of America
UTC	Universal Co-ordinated Time
VDL	VHF Digital Link
VFR	Visual Flight Rules
VHF	Very High Frequency (30 - 300 MHz)
VMC	Visual Meteorological Conditions
VOLMET	Meteorological Information for Aircraft in Flight
VOR	VHF Omni-directional Radio Range
VSAT	Very Small Aperture Terminal
WAAS	Wide Area Augmentation System (US)
WAFC	World Area Forecast Centre
WAFS	World Area Forecast System
WAN	Wide Area Network
WGS	World Geodetic Standard

© Eurocontrol, June 2004.

Index

A
A/G, 75
ACARS, 12
ADS, 18
ADSP, 18
AES, 76
AFTN, 18
AGT Data Link, 11
AGT Security, 11
AGT Threats, 11
Air Identification Tag, 23
AIT, 23
Alice, 29
AMCP, 18
AMHS, 14, 18
AMSS, 18
ANC, 17
APD, 46
ARINC, 14
ASPP, 18
ATM, 17
ATN, 17, 75, 93
ATN Security, 14
ATN security services, 13
ATN threats, 12
ATN vulnerability, 12
ATNP, 18
authentication, 94
    classical, 95
    digital signature, 97
    public-key, 96
    symmetric-key, 95

B
Bob, 29
BS, 50

C
CA, 22
Cascade, 31
CDMA, 52
Certificate authority, 22
Certificates Revocation List, 22
CIDIN, 18
CM, 18
CMA, 76
CNS, 17
CPDLC, 18
CRL, 22, 78
CW, 49

D
Data Link, 11
Data Link monitoring, 12
Denial of Service, 97
DLK, 11
DLK monitoring, 12
DoS, 97
DSP, 12

E
ESA, 55
Eurocontrol, 12
Eve, 29

F
FANS, 17
FDMA, 52
FIS, 18
FWHM, 49

G
G/G, 75
GEO, 51
GM, 17
GPS, 53
GS, 76

H
hash function, 96
HF Data Link, 18

I
ICAO, 14, 17
ICC, 18
IETF, 22
Internet Protocol, 22
IPSec, 23
IPv4, 22
IPv6, 22
IRDP, 13, 14
ISO, 17

L
LEO, 51

M
MEO, 51

N
NAT, 23

O
OACA, 22
OGS, 55
one-way function, 96
OSI, 17

© Eurocontrol, June 2004.

P
PAT, 55
PBS, 50
PKI, 13, 22, 76
PRMA, 52
protocol, 93
Public Key Infrastructure, 22

Q
QAP, 90
QBER, 28
QC, 45
QCKI, 78
QKD data relay, 78
QKD relay, 78
QKD: plain key, 30
QKD: raw key, 30
QoS, 23
qubit, 28, 30

R
Radio Frequency, 12
RF, 12

S
SARP, 17
security services, 13
SILEX, 55
SISCAS, 17

T
TDMA, 52

U
UAL, 18

V
Very High Frequency, 23
VHF, 23
VHF Data Link, 18
VPN, 89

 © Eurocontrol, June 2004.

Bibliography

[1] *"QuCrypt"*. Center for KvanteInformatik-University of Aarhus.

[2] "Le GPS au Service de la Sécurité Routière". 2004.

[3] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Identification and Entity Authentication*, chapter 10, pages 385–420. CRC Press edition, October 1996.

[4] Andrew G D Rowley. "The BB84 Protocol", June 2001.

[5] H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. "Experiment Quantum Cryptography". In *J. Cryptology*, volume 5, pages 3–28, May 1992.

[6] Bob Witulski. Key Management. In *Presentation at DLK Users Forum*, Brussels (Belgium), june 2003.

[7] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Lutherand, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons. "Practical Free-Space Quantum Key Distribution Over 1km". In *Phys. Rev. Lett.*, volume 81, pages 3283–3286, 1998.

[8] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson. "Daylight Quantum Key Distribution Over 1.6 km". In *Phys. Rev. Lett.*, volume 84, pages 5652–5655, June 2000.

[9] Charles Bennett and Gilles Brassard. "Quantum Cryptography: Public Key Distribution and Coin Tossing". In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, Bangalore (India), December 1984.

[10] Charles H. Bennett, Francois Bessettee, Gilles Brassard, Louis Salvail, and John Smolin. *"Experimental Quantum Cryptography"*, September 1991.

[11] Chip Elliott. *"Building The Quantum Networks"*. BBN Technolgies (USA), June 2002.

[12] Chip Elliott, Dr. David Pearson, and Dr. Gregory Troxel. "Quantum Cryptography in Practice". May 2003.

[13] Christoph Guenther. "The Relevance of Quantum Cryptography in Modern Cryptographic Systems". December 2003.

[14] Daniel Gottesman and Hoi-Kwong Lo. "Proof of Security of Quantum Key Distribution with Two-Way Classical Communications", September 2002.

© Eurocontrol, June 2004.

[15] Data Link Ad Hoc Committee. *"Ad Hoc Meeting on Security, Executive Summary for AEEC General Session 2002 Membership"*. ESC/GAD, Titan Corporation (Hanscom, MA, USA), may 2002.

[16] Dominic Mayers. "Unconditional Security in Quantum Cryptography". 48:351–406, July 2002.

[17] Dung Dang Minh and Michel Riguidel. "Usage of Secure Networks built using Quantum Technology". 2004.

[18] B. R. Elbert. *"The Satellite Communication Applications Handbook"*. Artech House, Inc, MA, 2002.

[19] N. Gisin, G. Ribordy, W. Tittle, and H. Zbinden. "Quantum Cryptography". In *Reviews of Modern Physics*, volume 74, pages 145–195, January 2002.

[20] P. M Gorman, P. R. Tapster, and J. G. Rarity. "Secure Free-Space Key Exchange To 1.9 km And Beyond". In *J. Mod. Opt. of Physics*, volume 48, pages 1887–1901, 2001.

[21] Guihua Zeng and Guangcan Guo. "Quantum Authentication Protocol". January 2000.

[22] Hitoshi Inamori, Norbert Lütkenhaus, and Dominic Mayers. "Unconditional Security of Practical Quantum Key Distribution". July 2001.

[23] Hoi-Kwong Lo. "Communication Complexity and Security of Quantum Key Distribution". April 2004.

[24] Horst Hering, Martin Hagmüller, and Gernot Kubin. "Safety and Security Increase for ATM through Unnoticeable Watermark Aircraft Identification Tag Transmitted with the VHF Voice Communication". In *Proceedings of the 22nd Digital Avionics Systems Conference (DASC)*, Indianapolis (USA), october 2003.

[25] Horst Hering, Martin Hagmüller, and Gernot Kubin. "Watermark Technology for the VHF Voice Communication". In Vu Duong, editor, *Eurocontrol Experimental Centre – 2003 Innovative Research Activity Report*, pages 93–103, Eurocontrol, Brétigny (France), may 2004.

[26] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson. "Practical Free-Space Quantum Key Distribution Over 10 km In Daylight And At Night". In *New Journal of Physics*, volume 4, pages 43.1–43.14, 2002.

[27] ICAO. *"Manual of Technical Provisions for the Aeronautical Telecommunications Network (ATN) - Standard and Recommended Practices (SARPs)"*, Mars 2001.

[28] Jaeook Lee and Sun Kang. "Satellite over Satellite (sos) Network: A Novel Architecture for Satellite Network".

[29] Jim McMath. *"Aeronautical Telecommunications Network (ATN): Security, Key Management and Distribution Security, Key Management and Distribution"*. AEEC Data Link Users Forum (Miami, FL, USA) and ESC/GAD, Titan Corporation (Hanscom, MA, USA), Public Release: 03-0052 edition, february 2003.

 © Eurocontrol, June 2004.

[30] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura. "Single-Photon Interference Over 150-km Transmission Using Silica-Based Integrated-Optic Interferometers For Quantum Cryptography Criterion". In *Submitted to Electronics Letters*, 2004.

[31] C. Kurtsiefer, P. Zarda, M. Halder, P. Gorman, P. Tapster, J. Rarity, and H. Weinfurter. "Long Distance Free-Space Quantum Cryptography". In *New Journal of Physics*, volume 4, pages 43.1–43.14, 2002.

[32] C. Kurtsiefer, P. Zarda, M. Halder, P. Gorman, P. Tapster, J. Rarity, and H. Weinfurter. "Long Distance Free-Space Quantum Cryptography", 2002.

[33] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. Gorman, P. Tapster, and J. Rarity. "A Step Towards Global Key Distribution". In *Nature*, volume 419, page 450, 2002.

[34] Lo Hoi Kwong and Chau HF. "Unconditional Security of Quantum Key Distribution over Abitrarily Long Distance". pages 2050–2056, 1999.

[35] Martin Pfennigbauer, Walter R Leeb, Markus Aspelmeyer, Thomas Jennewein, and Anton Zeilinger. "Free-Space Optical Quantum Key Distribution Using Intersatellite Link", november 2003.

[36] Minh-Dung Dang and Hong-Quang Nguyen. "A new Authentication Scheme for Quantum Key Distribution". 2005.

[37] Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum Cryptography. 74, March 2002.

[38] Nikolaos K. Papanikolaou. "Formal Specification and Verification of Quantum Cryptographic Protocols". Technical report, 2003.

[39] Oliver Gradon. "Quantum Key Travels Record Distance". october 2002.

[40] Patrick Bellot, Minh Dung Dang, and Hong Quang Nguyen. "A New Authentication Scheme for Quantum Key Distribution". 2004.

[41] Peter W. Shor and John Preskill. "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol". April 2004.

[42] A. Poppe, A. Ferrizzi, T. Lorünser, O. Maurhardt, R. Ursin, H. R. Böhm, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger. "Practical Quantum Key Distribution with Polarization Entangled Photons". July 2004.

[43] J G Rarty, P R Tapster, P M Gorman, and P Knight. "Ground to Satellite Secure Key Exchange Using Quantum Cryptography". 4(82), october 2002.

[44] Roy Oishi. *"ARINC IA Project Initiation/Modification (APIM)"*. february 2003.

[45] Roy Oishi. *ARINC IA Project Initiation/Modification (APIM)*. february 2003.

[46] Tom McParland, BCI, and Egg Harbor Township. "Public Key Infrastructure for Air Traffic Management Systems". 2001.